

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C. 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 20 December 1999 (20.12.99)	
International application No. PCT/ES99/00115	Applicant's or agent's file reference
International filing date (day/month/year) 30 April 1999 (30.04.99)	Priority date (day/month/year) 07 May 1998 (07.05.98)
Applicant FERRE HERRERO, Angel José	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
13 November 1999 (13.11.99)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

Lazar Joseph Panakal

Facsimile No.: (41-22) 740.14.35

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

REC'D 11 AUG 2000

WIPO

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference ES/MG	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/ES99/00115	International filing date (day/month/year) 30/04/1999	Priority date (day/month/year) 07/05/1998
International Patent Classification (IPC) or national classification and IPC H04L9/20		
Applicant FERRE HERRERO, Angel José		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.


2. This REPORT consists of a total of 6 sheets, including this cover sheet.

- ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 16 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 13/11/1999	Date of completion of this report 09.08.00
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Snell, T Telephone No. +49 89 2399 8802



**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/ES99/00115

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1,2,4,5,7-9, as originally filed
11-27

3,3A,6,6A,10,10A, as received on 26/05/2000 with letter of 24/05/2000
28

Claims, No.:

1-34 as received on 26/05/2000 with letter of 24/05/2000

Drawings, sheets:

1/12-12/12 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☒ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

see separate sheet

4. Additional observations, if necessary:

|

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/ES99/00115

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-34
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-34
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-34
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Cited documents

D1: US-A-5214703

D2: US-A-3798360

Re Item I

Basis of the report

1. The removal of the limitation in independent claims 1-4 and 23-26 "encrypting-decrypting device in patent US No. 5214703" from the independent claims and its replacement by the term "staged encryption device" has added subject-matter going beyond the disclosure in the application documents as originally filed, firstly as there is no support in the originally filed application for a generalisation to this degree, and secondly as it is unclear what the precise scope to be conferred to the term "staged encrypting-decrypting device" is. Even if US 5214703 really were implicitly a staged device, as alleged by the applicant, other types of device clearly fall within the scope of the term which were not at all envisaged in the application as originally filed. This amendment therefore contravenes Article 34(2)(b) PCT.

Re Item V

Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The invention relates to an encryption system based on a block encryption device, in particular the device described in patent US 5214703 (D1). Four independent claims 1-4 relate to a transmitting (ie encrypting) device. A further four independent claims 23-26 relate to corresponding receiving (ie decrypting) devices.
2. The problem with this type of encryption device is that the resulting ciphertext does not exhibit properties enabling an objective measure by the user of the device of the degree of diffusion and confusion of the plaintext. The aim of the invention is therefore to provide an encryption algorithm whereby the cipher text is randomised in such a way that allows the evaluation of the diffusion and confusion present in the encrypted data sequence given as output.

3. This problem is solved in accordance with the invention in that in addition to the key input Z applied to the encryption engine of the prior art, an additional key input is applied to a transforming block generating means and ex-OR combined with the plain text prior to being input to the encryption engine. The four independent claims 1, 3, 23 and 25 for an encryption device (figs 6, 8, 10 and 12 respectively) all embody this principle, as do in reverse fashion the decryption devices according to independent claims 2, 4, 24 and 26 (cf figs 7, 9, 11 and 13 respectively). The large number of independent claims is justified as it would be difficult and artificial to define these differing embodiments by means of dependent claims.
4. As regards inventive step, although D2 describes a similar principle, ie separate keys are applied to different parts of an algorithm, it would be difficult to apply the teaching of D2 to D1 without the benefit of hindsight, because the detail of the encryption algorithms is quite different; these systems are therefore not obviously compatible.

The subject-matter of independent claims 1-4 and 23-26 is therefore considered to be novel and to involve an inventive step (Articles 33(1)-(3) PCT). As in each case the independent claims relate to an apparatus, said subject-matter is also clearly industrially applicable (Article 33(4) PCT).

4. As claims 5-22 and 27-34 are all dependent on one or more of the independent claims, they also meet the requirements for novelty, inventive step and industrial applicability (Articles 33(1)-(4) PCT).

Re Item VII

Certain defects in the international application

1. The description on pages 6-8 should have been adapted to the new claims (Rule 5.1(a)(iii) PCT).

Re Item VIII

Certain observations on the international application

1. The claims should have been reformulated to clearly define the matter for which protection is sought (Article 6 PCT). Although there is no longer a reference to any document in the claims, the essential features of US 5214703 (which document was referred to in the claims as originally filed), which are defined in the present description on pages 9-11, should have been included in the independent claims.
2. The term "grouping" used in the claims is considered to be misleading, as the description and drawings refer to an exclusive-OR operation, ie a mathematical operation, whereas grouping implies only an association of data without any function being performed. The claims are therefore not clear (Article 6 PCT). The claims are also not supported by the description (Article 6 PCT), since despite the appearance of the term grouping in the description, the only concrete example given is an exclusive-OR operation, with no other suggestion of any other type of function. In this situation, objection arises, as explained in the PCT Guidelines III-6.5.
3. Although all claims are claims for an apparatus, some of the features are defined partially in terms of a use or in terms of actions (eg, in claim 1: "making use of a freely selectable control block", "an assembly means ... which assemble" etc), leading to a lack of clarity in construing the scope of protection (Article 84 EPC). The formulations "adapted to make use of ...", "an assembly means ... for assembling" should have been used (Article 6 PCT). A large number of features of the claims are deficient in this respect.
4. The intelligibility of the claims would have greatly benefitted from a linguistic revision, eg the first two lines of each the independent claims would have required commas to be intelligible (Article 6 PCT).

verify the mixture achieved in the resultant ciphertext in an objective way.

Mention must be given to patent U.S. No. 3,798,360 entitled "Step Code Ciphering System", invented by Horst Feistel, which makes use of an internal block cipher (22 in FIG. 1 of that patent) and part of the resulting ciphertext as input for the enciphering of the rest of the plaintext block. In the mentioned patent it is stated that "Each block cipher developed by a cryptographic device is comprised in part of data that has been twice enciphered by the same cryptographic device." and "A portion of the cipher text developed during the first encryption is stored and the remaining portion is re-enciphered in combination with new data bits to form a second ciphertext which is combined with the stored portion of the first cipher text to form a new composite block cipher that is transmitted.". The enciphering of the stream data is done on a block basis, being the basic feature of the system that each composite block cipher is formed by a portion of ciphertext that has been encrypted twice. Regarding the resulting ciphertext stream, such as the other abovementioned encrypting devices, this patent refers to an encrypting device whose resulting ciphertext stream presents no such properties to allow objective measures, by the user or the entity using the device, of the degree of diffusion and confusion of values presented in the mentioned ciphertext stream.

It is worth mentioning that as regards to the encryption key used for encrypting, for the time being, there exist recommendations about how it should be. Such recommendations are like those found in the Federal Information Processing Standards Publication 112 (FIPS PUB 112), which announces the standard "Password usage", dated from May 30, 1985, published by the "National Institute of Standards and Technology" ("NIST") of the Commerce Department of the US Government. Such recommendations refer to the "password" length, characters which are more advisable to use for its composition, and several limitations in its composition, amongst others. Cryptologists will recognize that passwords are related to encryption keys and are often used as such, as it is recommended in several sections of the same document FIPS PUB 112 such as section 3.9.3 entitled "Transmission" within chapter 3 entitled "Acceptable Basic Criteria"; another reference in the same direction can be found in section 3.7 entitled "Storage" within chapter 3 entitled "Factors" of Appendix A which is entitled "Password Usage Guidelines" as well as in other sections of said document.

The encryption key is one of the basic transforming elements of the plaintext in its encryption, since it is the combination of the operations plus the very operations performed by the encrypting device with the plaintext and the encryption key that yields the ciphertext. The encryption key used is one of the transforming elements, differential and variable in the series of transformations applied on the plaintext in order to produce the resultant ciphertext. The

encryption key impacts on the diffusion and confusion present in the ciphertext; thus, amongst all keys that can be used, there exist some which will introduce more diffusion and confusion of values than others in the resultant ciphertext. For the time being, there has never been a presentation of an encryption system which can return, as ciphertext resultant from its application, such a text that there is a measurable and objective way to discern, amongst all encryption keys that could be used, which one or ones produce more diffusion and confusion in the ciphertext resulting from each one.

Consequently, it can be stated that up to now, the same degree of invulnerability of a ciphertext, resulting from the application of a given encryption system, has been attributed to any ciphertext enciphered with any encryption key, based on the opinion of experts about the diffusion and confusion introduced by the used encryption systems. For the time being, encryption devices do not produce as a result a ciphertext with substantial properties to allow an objective measure of the diffusion and confusion present in the ciphertext.

The usage of encryption devices by laypersons is becoming very common, as in commercial electronic transactions or electronic mail amongst others, in which laypersons need

in the Federal Information Processing Standards Publication 81 (FIPS PUB 81), which announces the standard "DES Modes of Operation", by the "National Institute of Standards and Technology" ("NIST") of the Commerce Department of the United States Government, have been used in cryptology for quite a long time, they do not generate by themselves sequences substantially at random to which the application of randomness tests, as those mentioned above, was computationally feasible.

The system of this invention succeeds in generating substantially randomized encrypted data sequences by means of using the block encrypting device in patent US No. 5,214,703 entitled "Device for the conversion of a digital block and use of same", which is characterised by the encryption performed in successive stages, as described in the patent description. The staged encrypting-decrypting device performs both encryption of plaintext and decryption of ciphertext in successive stages. The system of this invention allows also the usage of a longer encryption key depending on the specific implementation of the invention.

According to this invention, the randomization-encryption device includes means for receiving as first input a data sequence and means for receiving as second input a control block. Said control block is divided by control block dividing means into two control initial blocks: control initial block of length G and control initial block of length $2N$. Generating means of encryption control subblocks with said control initial block of length $2N$ generate encryption control subblocks of length M . Transformer block generating means with said control initial block of length G , and with output block of length N whenever it is supplied, generate multitude of transformer blocks. Assembly means assemble data blocks of length N of said data sequence. Grouping means group corresponding said transformer block and corresponding said data block of length N resulting in interblock of length N . Said interblock of length N is supplied as input to the encrypting device in patent US No. 5,214,703 where it is grouped with said encryption control subblocks of length M , resulting in output block of length N . Said output block of length N is supplied as output of the randomizing-encrypting device object of this invention and is also supplied to said transformer block generating means which generate corresponding new transformer block for the randomization-encryption of the corresponding next data block of length N . Output means are supplied for transmitting the sequence of randomized-encrypted data consisting of output blocks of length N .

The device which is part of this invention for recovering the data sequence includes means for receiving at first input randomized-encrypted data sequence and means for receiving at second input control block. Said control block is divided by control block dividing means into two control initial blocks: control initial block of length G and control initial block of length $2N$.

M 25 05 00

6A

Generating means of decryption control subblocks with said control initial block of length $2N$ generate decryption control subblocks of length M . Transformer block generating means with said control initial block of length G and with randomized-encrypted data block of length N

5

AMENDED SHEET

ciphertext sequence Y arrives to the decrypting device 104, at the receiver's side, which feeds the target 105, a second computer for instance, with the plaintext sequence X. For encryption and decryption of data, the encrypting device 102 and the decrypting device 104 use a control block or encryption key Z. This encryption key Z is supplied from a key source 106 through channel 107 to the encrypting device 102 and through a secure channel 108, which can be a sealed mail for instance, to the decrypting device 104. The ciphertext sequence Y in the transmission channel 103 is always exposed to the risk that an enemy cryptanalyst 109 using the ciphertext sequence Y will try to obtain the plaintext sequence X or the encryption key Z (results of these attempts are designated by $\sim X$ and $\sim Z$).

For the time being, the concealment of the contents of the plaintext sequence X in the ciphertext sequence Y lies in the endorsement of diffusion and confusion introduced by the encrypting device used in front of enemy cryptanalyst regardless of the encryption key Z being used.

Figure 2 shows diagram of encrypting device 102 of Fig. 1, object of patent US No. 5,214,703, entitled "Device for the conversion of a digital block and use of same", corresponding with Fig. 2 of said patent report, and which has been included for later reference. The alphabetical references used in Fig. 2 are the same as those used in said Fig. 2 and description of patent US No. 5,214,703, so that it is easier to know the object they refer to. The numerical references have been modified in order to adapt them to this document. The encrypting device 102 encrypts the plaintext sequence X resulting in the ciphertext sequence Y by making use of control block Z, which arrives through channel 107. During the encryption process, control subblocks are encryption control subblocks Z_1 to Z_{52} , while during the decryption process they are decryption control subblocks U_1 to U_{52} , which are also derived from control block Z. In the exposition of the implementation methods of this invention, the control block Z will be referred to as control initial block Z. The term control block will be used to designate the randomization-encryption key of this invention. The method for obtaining the encryption control subblocks Z_1 to Z_{52} of the control block Z with the generator of encryption control subblocks 202 is described in said patent US No. 5,214,703 making use of same alphanumerical references.

The staged encrypting-decrypting device 204 needed for the encryption process $X \rightarrow Y$, where the encryption in successive stages is performed, is represented by a dashed line in Fig. 2 and will be subsequently referenced in that way.

M 25 05 00

10A

Figure 3 shows schematized diagram of the encrypting device 102 of Fig. 2 and includes

5

AMENDED SHEET

generates the transformer blocks WTJ from the fixed control initial block R, the same as the transformer block autonomous generator 5002 of Fig. 12. The control initial block R and the specific function F' that the transformer block autonomous generator 5002 implements are respectively equal to the used control initial block R and function F' implemented in the transformer block autonomous generator 5002 of the randomizing-encrypting device of Fig. 12 with which the randomized-encrypted text sequence Ys object of decryption was randomized-encrypted.

The complete description of the variation of decrypting device 502v3 is not done since it can be considered that the similarity with the descriptions offered in the methods of implementation of the decrypting devices of Fig. 7 and Fig. 12 with Fig. 13, together with the common references, allows the understanding of which is the method of implementation of this device.

INDUSTRIAL APPLICABILITY

The present invention is specially applicable in secret communications, maintenance of confidentiality of information, electronic commerce transactions, electronic mail communications and alike.

The specific implementation of the invention can be performed in many different ways and can depend on several factors like their application, the environment, the available and used technology, etcetera. A software implementation executed on electronic computers is possible. On the other hand, a hardware implementation can be possible where the elemental logic functions are in form of independent circuit units that can be built using discrete chip elements or preferably of several modules of very large scale integration (VLSI); microprocessors using "Read Only Memory" (ROM), or "Programmable Read Only Memory" (PROM), or "Electronically Erasable Read Only Memory" (EEROM) amongst many possible implementations. The hardware implementation has the advantage over the software implementation than can work substantially faster.

~~Everything that does not affect, alter, change or modify the essence of the described invention will be variable to the effects of this patent application, as well as the purpose is to claim the widest aspects of the invention in the widest possible way that the applicant knows at this time.~~

CLAIMS

1. Data sequence randomization-encryption system that making use of freely selectable control block with plaintext sequence generates substantially at random sequence , comprising:

- 5 a first input means for receiving a plaintext sequence (X),
- a second input means for receiving a control block (Kp),
- an assembly means of blocks of length N (301) which assemble said plaintext sequence (X) in a plurality of plaintext blocks (XI),
- a control block dividing means (1001) which divide said control block (Kp) into a
- 10 control initial block of length G (R) and a control initial block of length $2N$ (Z),
- a transformer block generating means (1002) which with said control initial block of length G (R) and a plurality corresponding randomized-encrypted text block (YI) generate a plurality of transformer blocks (WTI),
- a generating means of encryption control subblocks (202) which with said control
- 15 initial block of length $2N$ (Z) generate a plurality of encryption control subblocks (Z_1 - Z_{52}),
- a grouping means (603) which group corresponding said plaintext block (XI) and corresponding said transformer block (WTI), generating a grouped interblock (VI),
- a staged encrypting-decrypting means (204) which encrypt said grouped interblock (VI) with said plurality of encryption control subblocks (Z_1 - Z_{52}), generating said
- 20 randomized-encrypted text block (YI),
- an output supplying means (302) which supply plurality said randomized-encrypted text block (YI) making up a randomized-encrypted text sequence (Yp),
- whereby said randomized-encrypted text sequence (Yp) corresponds to said plaintext sequence (X) received by said first input means.

25 2. Data sequence randomization-encryption system that making use of control block from randomized-encrypted text sequence recovers plaintext sequence, comprising:

- a first input means for receiving a randomized-encrypted text sequence (Ys),
- a second input means for receiving a control block (Ks),
- 30 an assembly means of blocks of length N (301) which assemble said randomized-encrypted text sequence (Ys) in a plurality of randomized-encrypted text blocks (YJ),
- a control block dividing means (1001) which divide said control block (Ks) into a control initial block of length G (R) and a control initial block of length $2N$ (Z),
- a transformer block generating means (1002) which with said control initial block of

length G (R) and plurality corresponding previous said randomized-encrypted text block (YJ) assembled in said assembly means of blocks of length N (301) generate a plurality of transformer blocks (WTJ),

a generating means of decryption control subblocks (401) which with said control initial block of length $2N$ (Z) generate a plurality of decryption control subblocks (U_1-U_{52}),

a staged encrypting-decrypting means (204) which decrypt said randomized-encrypted text block (YJ) with said plurality of decryption control subblocks (U_1-U_{52}), generating a decrypted interblock (SJ),

a grouping means (603) which group said decrypted interblock (SJ) and said transformer block (WTJ), generating a plaintext block (XJ),

an output supplying means (302) which supply plurality said plaintext block (XJ) making up a plaintext sequence (X),

whereby said plaintext sequence (X) corresponds to said randomized-encrypted text sequence (Ys) received by said first input means.

3. Data sequence randomization-encryption system that making use of control initial block of length $2N$ freely selectable with plaintext sequence generates substantially at random sequence, comprising:

a first input means for receiving a plaintext sequence (X),

a second input means for receiving a control initial block of length $2N$ (Z),

an assembly means of blocks of length N (301) which assemble said plaintext sequence (X) in a plurality of plaintext blocks (XI),

a transformer block generating means (1002) which with a control initial block of length G (R) and a plurality corresponding randomized-encrypted text blocks (YI) generate a plurality of transformer blocks (WTI),

a generating means of encryption control subblocks (202) which with said control initial block of length $2N$ (Z) generate a plurality of encryption control subblocks (Z_1-Z_{52}),

a grouping means (603) which group corresponding said plaintext block (XI) and corresponding said transformer block (WTI), generating a grouped interblock (VI),

a staged encrypting-decrypting means (204) which encrypt said grouped interblock (VI) with said plurality of encryption control subblocks (Z_1-Z_{52}), generating said randomized-encrypted text block (YI),

an output supplying means (302) which supply plurality said randomized-encrypted

text block (YI) making up a randomized-encrypted text sequence (Yp),
 whereby said randomized-encrypted text sequence (Yp) corresponds to said plaintext sequence (X) received by said first input means.

5 4. Data sequence randomization-encryption system that making use of control initial block of length $2N$ from randomized-encrypted text sequence recovers plaintext sequence, comprising:

a first input means for receiving a randomized-encrypted text sequence (Ys),

a second input means for receiving a control initial block of length $2N$ (Z),

10 an assembly means of blocks of length N (301) which assemble said randomized-encrypted text sequence (Ys) in a plurality of randomized-encrypted text blocks (YJ),

a transformer block generating means (1002) which with a control initial block of length G (R) and plurality corresponding previous said randomized-encrypted text block (YJ) assembled in said assembly means of blocks of length N (301) generate a plurality of transformer blocks (WTJ),

15 a generating means of decryption control subblocks (401) which with said control initial block of length $2N$ (Z) generate a plurality of decryption control subblocks (U_1 - U_{s2}),

20 a staged encrypting-decrypting means (204) which decrypt said randomized-encrypted text block (YJ) with said plurality of decryption control subblocks (U_1 - U_{s2}), generating a decrypted interblock (SJ),

a grouping means (603) which group said decrypted interblock (SJ) and said transformer block (WTJ), generating a plaintext block (XJ),

an output supplying means (302) which supply plurality said plaintext block (XJ) making up a plaintext sequence (X),

25 whereby said plaintext sequence (X) corresponds to said randomized-encrypted text sequence (Ys) received by said first input means.

30 5. The system of claim 1 or 2 or 3 or 4 wherein said transformer block generating means (1002) generate said transformer block (WTI;WTJ) implementing a function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)).

6. The system of claim 5 wherein said grouping means (603) include an exclusive-OR operation.

7. The system of claim 6 wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)) for nth said transformer block (WTI;WTJ) equal to nth block of length N generated by a function E_n (said control initial block of length G (R)) XOR nth minus one said randomized-encrypted text block (YI;YJ).

8. The system of claim 7 wherein said transformer block generating means (1002) implement said function E_n (said control initial block of length G (R)) as $E_n(R_i) = (E_{n-1}(R_i) \text{ oper } B) \bmod 2^{Q_i}$, wherein said Q_i less than or equal to 64, said R_i of length said Q_i is subblock of said control initial block of length G (R), said oper arithmetic operation selected from the group consisting of addition and subtraction and shift, said B a value, said mod module operation.

9. The system of claim 8 wherein said control initial block of length 2N (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.

10. The system of claim 7 wherein said transformer block generating means (1002) implement said function E_n (said control initial block of length G (R)) including a random number generator.

11. The system of claim 10 wherein said control initial block of length 2N (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of seed length of said random number generator.

12. The system of claim 7 wherein said transformer block generating means (1002) implement said function E_n (said control initial block of length G (R)) including a hash function.

13. The system of claim 12 wherein said control initial block of length 2N (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of zero or more bits.

14. The system of claim 6 wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)) as

AMENDED SHEET

for first said transformer block (WTI;WTJ) includes said control initial block of length G (R),

for nth said transformer block (WTI;WTJ) is equal to nth minus one said randomized-encrypted text block (YI;YJ) XOR nth minus one said transformer block (WTI;WTJ).

5

15. The system of claim 14 wherein said control initial block of length 2N (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.

10

16. The system of claim 6 wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)) as

for first said transformer block (WTI;WTJ) is said control initial block of length G (R),

for nth said transformer block (WTI;WTJ) is nth minus one said randomized-encrypted text block (YI;YJ).

15

17. The system of claim 16 wherein said control initial block of length 2N (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.

20

18. The system of claim 6 wherein said transformer block generating means (1002) implement said function H (said control initial block of length G (R), said randomized-encrypted text block (YI;YJ)) for nth said transformer block (WTI;WTJ) equal to nth block of length N generated by a function E_n (nth minus one said randomized-encrypted text block (YI;YJ)) XOR said control initial block of length G (R).

25

19. The system of claim 18 wherein said transformer block generating means (1002) implement said function E_n (nth minus one said randomized-encrypted text block (YI;YJ)) as $E_n(Y_i) = (E_{n-1}(Y_i) \text{ oper } B) \bmod 2^{Q_i}$, wherein said Q_i less than or equal to 64, said Y_i of length said Q_i is subblock of said nth minus one said randomized-encrypted text block (YI;YJ), said oper arithmetic operation selected from the group consisting of addition and subtraction and shift, said B a value, said mod module operation.

30

20. The system of claim 19 wherein said control initial block of length 2N (Z) made up

preferably of 128 bits and said control initial block of length $G(R)$ made up preferably of 64 bits.

21. The system of claim 18 wherein said transformer block generating means (1002)
 5 implement said function E_n (nth minus one said randomized-encrypted text block $(YI; YJ)$) including a hash function.

22. The system of claim 21 wherein said control initial block of length $2N(Z)$ made up
 preferably of 128 bits and said control initial block of length $G(R)$ made up preferably of zero
 10 or more bits.

23. Data sequence randomization-encryption system that making use of control block freely
 selectable with plaintext sequence generates substantially at random sequence, comprising:

a first input means for receiving a plaintext sequence (X) ,

15 a second input means for receiving a control block (Kp) ,

an assembly means of blocks of length $N(301)$ which assemble said plaintext sequence
 (X) in a plurality of plaintext blocks (XI) ,

a control block dividing means (1001) which divide said control block (Kp) into a
 control initial block of length $G(R)$ and a control initial block of length $2N(Z)$,

20 a transformer block autonomous generating means (5002) which with said control
 initial block of length $G(R)$ generate a plurality of transformer blocks (WTI) ,

a generating means of encryption control subblocks (202) which with said control
 initial block of length $2N(Z)$ generate a plurality of encryption control subblocks (Z_1-Z_{52}) ,

25 a grouping means (603) which group corresponding said plaintext block (XI) and
 corresponding said transformer block (WTI) , generating a grouped interblock (VI) ,

a staged encrypting-decrypting means (204) which encrypt said grouped interblock
 (VI) with said plurality of encryption control subblocks (Z_1-Z_{52}) , generating a randomized-
 encrypted text block (YI) ,

30 an output supplying means (302) which supply plurality said randomized-encrypted
 text block (YI) making up a randomized-encrypted text sequence (Yp) ,
 whereby said randomized-encrypted text sequence (Yp) corresponds to said plaintext sequence
 (X) received by said first input means.

24. Data sequence randomization-encryption system that making use of control block from

randomized-encrypted text sequence recovers plaintext sequence, comprising:

- a first input means for receiving a randomized-encrypted text sequence (\underline{Ys}),
 - a second input means for receiving a control block (Ks),
 - an assembly means of blocks of length N (301) which assemble said randomized-encrypted text sequence (\underline{Ys}) in a plurality of randomized-encrypted text blocks (YJ),
 - a control block dividing means (1001) which divide said control block (Ks) into a control initial block of length G (R) and a control initial block of length $2N$ (Z),
 - a transformer block autonomous generating means (5002) which with said control initial block of length G (R) generate a plurality of tranformer blocks (WTJ),
 - a generating means of decryption control subblocks (401) which with said control initial block of length $2N$ (Z) generate a plurality of decryption control subblocks (U_1-U_{52}),
 - a staged encrypting-decrypting means (204) which decrypt said randomized-encrypted text block (YJ) with said plurality of decryption control subblocks ($U_1 - U_{52}$), generating a decrypted interblock (SJ),
 - a grouping means (603) which group said decrypted interblock (SJ) and said transformer block (WTJ), generating a plaintext block (XJ),
 - an output supplying means (302) which supply plurality said plaintext block (XJ) making up a plaintext sequence (\underline{X}),
- whereby said plaintext sequence (\underline{X}) corresponds to said randomized-encrypted text sequence (\underline{Ys}) received by said first input means.

25. Data sequence randomization-encryption system that making use of control initial block of length $2N$ freely selectable with plaintext sequence generates substantially at random sequence, comprising:

- a first input means for receiving a plaintext sequence (\underline{X}),
- a second input means for receiving a control initial block of length $2N$ (Z),
- an assembly means of blocks of length N (301) which assemble said plaintext sequence (\underline{X}) in a plurality of plaintext blocks (XI),
- a transformer block autonomous generating means (5002) which with a control initial block of length G (R) generate a plurality of transformer blocks (WTI),
- a generating means of encryption control subblocks (202) which with said control initial block of length $2N$ (Z) generate a plurality of encryption control subblocks (Z_1-Z_{52}),
- a grouping means (603) which group corresponding said plaintext block (XI) and

corresponding said transformer block (WTI), generating a grouped interblock (VI),

a staged encrypting-decrypting means (204) which encrypt said grouped interblock (VI) with said plurality of encryption control subblocks (Z_1 - Z_{52}), generating a randomized-encrypted text block (YI),

an output supplying means (302) which supply plurality said randomized-encrypted text block (YI) making up a randomized-encrypted text sequence ($\underline{Y_p}$),
whereby said randomized-encrypted text sequence ($\underline{Y_p}$) corresponds to said plaintext sequence (\underline{X}) received by said first input means.

26. Data sequence randomization-encryption system that making use of control initial block of length $2N$ from randomized-encrypted text sequence recovers plaintext sequence, comprising:

a first input means for receiving a randomized-encrypted text sequence ($\underline{Y_s}$),

a second input means for receiving a control initial block of length $2N$ (Z),

an assembly means of blocks of length N (301) which assemble said randomized-encrypted text sequence ($\underline{Y_s}$) in a plurality of randomized-encrypted text blocks (YJ),

a transformer block autonomous generating means (5002) which with a control initial block of length G (R) generate a plurality of transformer blocks (WTJ),

a generating means of decryption control subblocks (401) which with said control initial block of length $2N$ (Z) generate a plurality of decryption control subblocks (U_1 - U_{52}),

a staged encrypting-decrypting means (204) which decrypt said randomized-encrypted text block (YJ) with said plurality of decryption control subblocks (U_1 - U_{52}), generating a decrypted interblock (SJ),

a grouping means (603) which group said decrypted interblock (SJ) and said transformer block (WTJ), generating a plaintext block (XJ),

an output supplying means (302) which supply plurality said plaintext block (XJ) making up a plaintext sequence (\underline{X}),

whereby said plaintext sequence (\underline{X}) corresponds to said randomized-encrypted text sequence ($\underline{Y_s}$) received by said first input means.

27. The system of claim 23 or 24 or 25 or 26 wherein said tranformer block autonomous generating means (5002) generate said transformer block (WTI;WTJ) implementing a function H (said control initial block of length G (R)).

28. The system of claim 27 wherein said grouping means (603) include an exclusive-OR operation.

29. The system of claim 28 wherein said transformer block autonomous generating means (5002) implement said function H (said control initial block of length G (R)) for nth said transformer block (WTI;WTJ) as $H_n(R_i) = (H_{n-1}(R_i) \text{ oper } B) \bmod 2^{Q_i}$, wherein said Q_i less than or equal to 64, said R_i of length said Q_i is subblock of said control initial block of length G (R), said oper arithmetic operation selected from the group consisting of addition and subtraction and shift, said B a value, said mod module operation.

30. The system of claim 29 wherein said control initial block of length 2N (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of 64 bits.

31. The system of claim 28 wherein said transformer block autonomous generating means (5002) implement said function H (said control initial block of length G (R)) including a random number generator.

32. The system of claim 31 wherein said control initial block of length 2N (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of seed length of said random number generator.

33. The system of claim 28 wherein said transformer block autonomous generating means (5002) implement said function H (said control initial block of length G (R)) including a hash function.

34. The system of claim 33 wherein said control initial block of length 2N (Z) made up preferably of 128 bits and said control initial block of length G (R) made up preferably of zero or more bits.

AMENDED SHEET

verify the mixture achieved in the resultant ciphertext in an objective way.

It is worth mentioning that as regards to the encryption key used for encrypting, for the time being, there exist recommendations about how it should be. Such recommendations are like those found in the Federal Information Processing Standards Publication 112 (FIPS PUB 112), which announces the standard "Password usage", dated from May 30, 1985, published by the "National Institute of Standards and Technology" ("NIST") of the Commerce Department of the US Government. Such recommendations refer to the "password" length, characters which are more advisable to use for its composition, and several limitations in its composition, amongst others. Cryptologists will recognize that passwords are related to encryption keys and are often used as such, as it is recommended in several sections of the same document FIPS PUB 112 such as section 3.9.3 entitled "Transmission" within chapter 3 entitled "Acceptable Basic Criteria"; another reference in the same direction can be found in section 3.7 entitled "Storage" within chapter 3 entitled "Factors" of Appendix A which is entitled "Password Usage Guidelines" as well as in other sections of said document.

The encryption key is one of the basic transforming elements of the plaintext in its encryption, since it is the combination of the operations plus the very operations performed by the encrypting device with the plaintext and the encryption key that yields the ciphertext. The encryption key used is one of the transforming elements, differential and variable in the series of transformations applied on the plaintext in order to produce the resultant ciphertext. The encryption key impacts on the diffusion and confusion present in the ciphertext; thus, amongst all keys that can be used, there exist some which will introduce more diffusion and confusion of values than others in the resultant ciphertext. For the time being, there has never been a presentation of an encryption system which can return, as ciphertext resultant from its application, such a text that there is a measurable and objective way to discern, amongst all encryption keys that could be used, which one or ones produce more diffusion and confusion in the ciphertext resulting from each one.

Consequently, it can be stated that up to now, the same degree of invulnerability of a ciphertext, resulting from the application of a given encryption system, has been attributed to any ciphertext enciphered with any encryption key, based on the opinion of experts about the diffusion and confusion introduced by the used encryption systems. For the time being, encryption devices do not produce as a result a ciphertext with substantial properties to allow an objective measure of the diffusion and confusion present in the ciphertext.

The usage of encryption devices by laypersons is becoming very common, as in commercial electronic transactions or electronic mail amongst others, in which laypersons need

in the Federal Information Processing Standards Publication 81 (FIPS PUB 81), which announces the standard "DES Modes of Operation", by the "National Institute of Standards and Technology" ("NIST") of the Commerce Department of the United States Government, have been used in cryptology for quite a long time, they do not generate by themselves sequences substantially at random to which the application of randomness tests, as those mentioned above, was computationally feasible.

The system of this invention succeeds in generating substantially randomized encrypted data sequences by means of using the block encrypting device in patent US No. 5,214,703 entitled "Device for the conversion of a digital block and use of same". This system allows also the usage of a longer encryption key depending on the specific implementation of the invention.

According to this invention, the randomization-encryption device includes means for receiving as first input a data sequence and means for receiving as second input a control block. Said control block is divided by control block dividing means into two control initial blocks: control initial block of length G and control initial block of length $2N$. Generating means of encryption control subblocks with said control initial block of length $2N$ generate encryption control subblocks of length M . Transformer block generating means with said control initial block of length G , and with output block of length N whenever it is supplied, generate multitude of transformer blocks. Assembly means assemble data blocks of length N of said data sequence. Grouping means group corresponding said transformer block and corresponding said data block of length N resulting in interblock of length N . Said interblock of length N is supplied as input to the encrypting device in patent US No. 5,214,703 where it is grouped with said encryption control subblocks of length M , resulting in output block of length N . Said output block of length N is supplied as output of the randomizing-encrypting device object of this invention and is also supplied to said transformer block generating means which generate corresponding new transformer block for the randomization-encryption of the corresponding next data block of length N . Output means are supplied for transmitting the sequence of randomized-encrypted data consisting of output blocks of length N .

The device which is part of this invention for recovering the data sequence includes means for receiving at first input randomized-encrypted data sequence and means for receiving at second input control block. Said control block is divided by control block dividing means into two control initial blocks: control initial block of length G and control initial block of length $2N$. Generating means of decryption control subblocks with said control initial block of length $2N$ generate decryption control subblocks of length M . Transformer block generating means with said control initial block of length G and with randomized-encrypted data block of length N

ciphertext sequence Y arrives to the decrypting device 104, at the receiver's side, which feeds the target 105, a second computer for instance, with the plaintext sequence X. For encryption and decryption of data, the encrypting device 102 and the decrypting device 104 use a control block or encryption key Z. This encryption key Z is supplied from a key source 106 through channel 107 to the encrypting device 102 and through a secure channel 108, which can be a sealed mail for instance, to the decrypting device 104. The ciphertext sequence Y in the transmission channel 103 is always exposed to the risk that an enemy cryptanalyst 109 using the ciphertext sequence Y will try to obtain the plaintext sequence X or the encryption key Z (results of these attempts are designated by $\sim X$ and $\sim Z$).

For the time being, the concealment of the contents of the plaintext sequence X in the ciphertext sequence Y lies in the endorsement of diffusion and confusion introduced by the encrypting device used in front of enemy cryptanalyst regardless of the encryption key Z being used.

Figure 2 shows diagram of encrypting device 102 of Fig. 1, object of patent US No. 5,214,703, entitled "Device for the conversion of a digital block and use of same", corresponding with Fig. 2 of said patent report, and which has been included for later reference. The alphabetical references used in Fig. 2 are the same as those used in said Fig. 2 and description of patent US No. 5,214,703, so that it is easier to know the object they refer to. The numerical references have been modified in order to adapt them to this document. The encrypting device 102 encrypts the plaintext sequence X resulting in the ciphertext sequence Y by making use of control block Z, which arrives through channel 107. During the encryption process, control subblocks are encryption control subblocks Z_1 to Z_{52} , while during the decryption process they are decryption control subblocks U_1 to U_{52} , which are also derived from control block Z. In the exposition of the implementation methods of this invention, the control block Z will be referred to as control initial block Z. The term control block will be used to designate the randomization-encryption key of this invention. The method for obtaining the encryption control subblocks Z_1 to Z_{52} of the control block Z with the generator of encryption control subblocks 202 is described in said patent US No. 5,214,703 making use of same alphanumerical references.

The encrypting-decrypting device 204 needed for the encryption process $X \rightarrow Y$ is represented by a dashed line in Fig. 2 and will be subsequently referenced in that way.

Figure 3 shows schematized diagram of the encrypting device 102 of Fig. 2 and includes

generates the transformer blocks WTJ from the fixed control initial block R, the same as the transformer block autonomous generator 5002 of Fig. 12. The control initial block R and the specific function F' that the transformer block autonomous generator 5002 implements are respectively equal to the used control initial block R and function F' implemented in the transformer block autonomous generator 5002 of the randomizing-encrypting device of Fig. 12 with which the randomized-encrypted text sequence Ys object of decryption was randomized-encrypted.

The complete description of the variation of decrypting device 502v3 is not done since it can be considered that the similarity with the descriptions offered in the methods of implementation of the decrypting devices of Fig. 7 and Fig. 12 with Fig. 13, together with the common references, allows the understanding of which is the method of implementation of this device.

INDUSTRIAL APPLICABILITY

The present invention is specially applicable in secret communications, maintenance of confidentiality of information, electronic commerce transactions, electronic mail communications and alike.

The specific implementation of the invention can be performed in many different ways and can depend on several factors like their application, the environment, the available and used technology, etcetera. A software implementation executed on electronic computers is possible. On the other hand, a hardware implementation can be possible where the elemental logic functions are in form of independent circuit units that can be built using discrete chip elements or preferably of several modules of very large scale integration (VLSI); microprocessors using "Read Only Memory" (ROM), or "Programmable Read Only Memory" (PROM), or "Electronically Erasable Read Only Memory" (EEPROM) amongst many possible implementations. The hardware implementation has the advantage over the software implementation than can work substantially faster.

Everything that does not affect, alter, change or modify the essence of the described invention will be variable to the effects of this patent application; as well as the purpose is to claim the widest aspects of the invention in the widest possible way that the applicant knows at this time.

CLAIMS

1. Data sequence randomization-encryption system that making use of freely selectable control block with plaintext sequence generates substantially at random sequence , comprising:

5 first input means for receiving plaintext sequence,
 second input means for receiving control block,
 assembly means of blocks of length N which assemble said plaintext sequence in
multitude of plaintext blocks,
 control block dividing means which divide said control block into control initial block
10 of length G and control initial block of length $2N$,
 transformer block generating means which with said control initial block of length G
and multitude corresponding randomized-encrypted text block generate multitude of
transformer blocks,
 generating means of encryption control subblocks which with said control initial block
15 of length $2N$ generate plurality of encryption control subblocks,
 grouping means which group corresponding said plaintext block and corresponding
said transformer block, generating grouped interblock,
 encrypting-decrypting means which encrypt said grouped interblock with said plurality
of encryption control subblocks, generating said randomized-encrypted text block,
20 wherein said encrypting-decrypting means include encrypting-decrypting device in patent
US No. 5,214,703,
 output supplying means which supply multitue said randomized-encrypted text block
making up randomized-encrypted text sequence,
whereby said randomized-encrypted text sequence corresponds to said plaintext sequence
25 received by said first input means,
whereby said randomized-encrypted text sequence is substantially at random,
whereby the diffusion and confusion of values of said randomized-encrypted text sequence is
objectively measurable,
whereby the diffusion and confusion of values introduced by said control block received by said
30 second input means is measurable.

2. Data sequence randomization-encryption system that making use of control block from randomized-encrypted text sequence recovers plaintext sequence, comprising:

 first input means for receiving randomized-encrypted text sequence,

second input means for receiving control block,
 assembly means of blocks of length N which assemble said randomized-encrypted text
 sequence in multitude of randomized-encrypted text blocks,
 control block dividing means which divide said control block into control initial block
 5 of length G and control initial block of length $2N$,
 transformer block generating means which with said control initial block of length G
 and multitude corresponding previous said randomized-encrypted text block assembled in
 said assembly means of blocks of length N generate multitude of transformer blocks,
 generating means of decryption control subblocks which with said control initial block
 10 of length $2N$ generate plurality of decryption control subblocks,
 encrypting-decrypting means which decrypt said randomized-encrypted text block with
 said plurality of decryption control subblocks, generating decrypted interblock, wherein
 said encrypting-decrypting means include encrypting-decrypting device in patent US
 No. 5,214,703,
 15 grouping means which group said decrypted interblock and said transformer block,
 generating plaintext block,
 output supplying means which supply multitude said plaintext block making up
 plaintext sequence,
 whereby said plaintext sequence corresponds to said randomized-encrypted text sequence
 20 received by said first input means.

3. Data sequence randomization-encryption system that making use of control initial block of
 length $2N$ freely selectable with plaintext sequence generates substantially at random sequence,
 comprising:

25 first input means for receiving plaintext sequence,
 second input means for receiving control initial block of length $2N$,
 assembly means of blocks of length N which assemble said plaintext sequence in
 multitude of plaintext blocks,
 transformer block generating means which with control initial block of length G and
 30 multitude corresponding randomized-encrypted text blocks generate multitude of
 transformer blocks,
 generating means of encryption control subblocks which with said control initial block
 of length $2N$ generate plurality of encryption control subblocks,
 grouping means which group corresponding said plaintext block and corresponding

said transformer block, generating grouped interblock,

encrypting-decrypting means which encrypt said grouped interblock with said plurality of encryption control subblocks, generating said randomized-encrypted text block, wherein said encrypting-decrypting means include encrypting-decrypting device in patent
5 US No. 5,214,703,

output supplying means which supply multitude said randomized-encrypted text block making up randomized-encrypted text sequence,

whereby said randomized-encrypted text sequence corresponds to said plaintext sequence received by said first input means,

10 whereby said randomized-encrypted text sequence is substantially at random,

whereby the diffusion and confusion of values of said randomized-encrypted text sequence is objectively measurable,

whereby the diffusion and confusion of values introduced by said control initial block of length $2N$ received by said second input means is measurable.

15

4. Data sequence randomization-encryption system that making use of control initial block of length $2N$ from randomized-encrypted text sequence recovers plaintext sequence, comprising:

first input means for receiving randomized-encrypted text sequence,

second input means for receiving control initial block of length $2N$,

20 assembly means of blocks of length N which assemble said randomized-encrypted text sequence in multitude of randomized-encrypted text blocks,

transformer block generating means which with control initial block of length G and multitude corresponding previous said randomized-encrypted text block assembled in said assembly means of blocks of length N generate multitude of transformer blocks,

25 generating means of decryption control subblocks which with said control initial block of length $2N$ generate plurality of decryption control subblocks,

encrypting-decrypting means which decrypt said randomized-encrypted text block with said plurality of decryption control subblocks, generating decrypted interblock, wherein said encrypting-decrypting means include encrypting-decrypting device in patent US
30 No. 5,214,703,

grouping means which group said decrypted interblock and said transformer block, generating plaintext block,

output supplying means which supply multitude said plaintext block making up plaintext sequence,

whereby said plaintext sequence corresponds to said randomized-encrypted text sequence received by said first input means.

5 5. The system of claim 1 or 2 or 3 or 4 wherein said transformer block generating means generate said transformer block implementing function H (said control initial block of length G, said randomized-encrypted text block).

6. The system of claim 5 wherein said grouping means include exclusive-OR operation.

10 7. The system of claim 6 wherein said transformer block generating means implement said function H (said control initial block of length G, said randomized-encrypted text block) for nth said transformer block equal to nth block of length N generated by function E_n (said control initial block of length G) XOR nth minus one said randomized-encrypted text block.

15 8. The system of claim 7 wherein said transformer block generating means implement said function E_n (said control initial block of length G) as $E_n(R_i) = (E_{n-1}(R_i) \text{ oper } B) \bmod 2^{Q_i}$, wherein said Q_i less than or equal to 64, said R_i of length said Q_i is subblock of said control initial block of length G, said oper arithmetic operation selected from the group consisting of addition and subtraction and shift, said B value, said mod module operation.

20 9. The system of claim 8 wherein said control initial block of length 2N made up preferably of 128 bits and said control initial block of length G made up preferably of 64 bits.

25 10. The system of claim 7 wherein said transformer block generating means implement said function E_n (said control initial block of length G) including random number generator.

30 11. The system of claim 10 wherein said control initial block of length 2N made up preferably of 128 bits and said control initial block of length G made up preferably of seed length of said random number generator.

12. The system of claim 7 wherein said transformer block generating means implement said function E_n (said control initial block of length G) including hash function.

13. The system of claim 12 wherein said control initial block of length 2N made up

preferably of 128 bits and said control initial block of length G made up preferably of zero or more bits.

14. The system of claim 6 wherein said transformer block generating means implement said function H (said control initial block of length G, said randomized-encrypted text block) as
 for first said transformer block includes said control initial block of length G,
 for nth said transformer block is equal to nth minus one said randomized-encrypted text block XOR nth minus one said transformer block.

15. The system of claim 14 wherein said control initial block of length 2N made up preferably of 128 bits and said control initial block of length G made up preferably of 64 bits.

16. The system of claim 6 wherein said transformer block generating means implement said function H (said control initial block of length G, said randomized-encrypted text block) as
 for first said transformer block is said control initial block of length G,
 for nth said transformer block is nth minus one said randomized-encrypted text block.

17. The system of claim 16 wherein said control initial block of length 2N made up preferably of 128 bits and said control initial block of length G made up preferably of 64 bits.

18. The system of claim 6 wherein said transformer block generating means implement said function H (said control initial block of length G, said randomized-encrypted text block) for nth said transformer block equal to nth block of length N generated by function E_n (nth minus one said randomized-encrypted text block) XOR said control initial block of length G.

19. The system of claim 18 wherein said transformer block generating means implement said function E_n (nth minus one said randomized-encrypted text block) as $E_n (YI_i) = (E_{n-1} (YI_i) \text{ oper } B) \bmod 2^{Q_i}$, wherein said Q_i less than or equal to 64, said YI_i of length said Q_i is subblock of said nth minus one said randomized-encrypted text block, said oper arithmetic operation selected from the group consisting of addition and subtraction and shift, said B value, said mod module operation.

20. The system of claim 19 wherein said control initial block of length 2N made up preferably of 128 bits and said control initial block of length G made up preferably of 64 bits.

21. The system of claim 18 wherein said transformer block generating means implement said function E_n (nth minus one said randomized-encrypted text block) including hash function.

22. The system of claim 21 wherein said control initial block of length $2N$ made up preferably of 128 bits and said control initial block of length G made up preferably of zero or more bits.

23. Data sequence randomization-encryption system that making use of control block freely selectable with plaintext sequence generates substantially at random sequence, comprising:

10 first input means for receiving plaintext sequence,
 second input means for receiving control block,
 assembly means of blocks of length N which assemble said plaintext sequence in multitude of plaintext blocks,
 control block dividing means which divide said control block into control initial block
 15 of length G and control initial block of length $2N$,
 transformer block autonomous generating means which with said control initial block of length G generate multitude of transformer blocks,
 generating means of encryption control subblocks which with said control initial block of length $2N$ generate plurality of encryption control subblocks,
 20 grouping means which group corresponding said plaintext block and corresponding said transformer block, generating grouped interblock,
 encrypting-decrypting means which encrypt said grouped interblock with said plurality of encryption control subblocks, generating randomized-encrypted text block, wherein said encrypting-decrypting means include encrypting-decrypting device in patent US
 25 No. 5,214,703,
 output supplying means which supply multitude said randomized-encrypted text block making up randomized-encrypted text sequence,
 whereby said randomized-encrypted text sequence corresponds to said plaintext sequence received by said first input means,
 30 whereby said randomized-encrypted text sequence is substantially at random,
 whereby the diffusion and confusion of values of said randomized-encrypted text sequence is objectively measurable,
 whereby the diffusion and confusion of values introduced by said control block received by said second input means is measurable.

24. Data sequence randomization-encryption system that making use of control block from randomized-encrypted text sequence recovers plaintext sequence, comprising:

first input means for receiving randomized-encrypted text sequence,

second input means for receiving control block,

5 assembly means of blocks of length N which assemble said randomized-encrypted text sequence in multitude of randomized-encrypted text blocks,

control block dividing means which divide said control block into control initial block of length G and control initial block of length $2N$,

10 transformer block autonomous generating means which with said control initial block of length G generate multitude of tranformer blocks,

generating means of decryption control subblocks which with said control initial block of length $2N$ generate plurality of decryption control subblocks,

15 encrypting-decrypting means which decrypt said randomized-encrypted text block with said plurality of decryption control subblocks, generating decrypted interblock, wherein said encrypting-decrypting means include encrypting-decrypting device in patent US No. 5,214,703,

grouping means which group said decrypted interblock and said transformer block, generating plaintext block,

20 output supplying means which supply multitude said plaintext block making up plaintext sequence,

whereby said plaintext sequence corresponds to said randomized-encrypted text sequence received by said first input means.

25 25. Data sequence randomization-encryption system that making use of control initial block of length $2N$ freely selectable with plaintext sequence generates substantially at random sequence, comprising:

first input means for receiving plaintext sequence,

second input means for receiving control initial block of length $2N$,

30 assembly means of blocks of length N which assemble said plaintext sequence in multitude of plaintext blocks,

transformer block autonomous generating means which with control initial block of length G generate multitude of transformer blocks,

generating means of encryption control subblocks which with said control initial block of length $2N$ generate plurality of encryption control subblocks,

grouping means which group corresponding said plaintext block and corresponding said transformer block, generating grouped interblock,

encrypting-decrypting means which encrypt said grouped interblock with said plurality of encryption control subblocks, generating randomized-encrypted text block, wherein
5 said encrypting-decrypting means include encrypting-decrypting device in patent US No. 5,214,703,

output supplying means which supply multitude said randomized-encrypted text block making up randomized-encrypted text sequence,

whereby said randomized-encrypted text sequence corresponds to said plaintext sequence
10 received by said first input means,

whereby said randomized-encrypted text sequence is substantially at random,

whereby the diffusion and confusion of values of said randomized-encrypted text sequence is objectively measurable,

whereby the diffusion and confusion of values introduced by said control initial block of length

15 $2N$ received by said second input means is measurable.

26. Data sequence randomization-encryption system that making use of control initial block of length $2N$ from randomized-encrypted text sequence recovers plaintext sequence, comprising:

first input means for receiving randomized-encrypted text sequence,

20 second input means for receiving control initial block of length $2N$,

assembly means of blocks of length N which assemble said randomized-encrypted text sequence in multitude of randomized-encrypted text blocks,

transformer block autonomous generating means which with control initial block of length G generate multitude of transformer blocks,

25 generating means of decryption control subblocks which with said control initial block of length $2N$ generate plurality of decryption control subblocks,

encrypting-decrypting means which decrypt said randomized-encrypted text block with said plurality of decryption control subblocks, generating decrypted interblock, wherein said encrypting-decrypting means include encrypting-decrypting device in patent US
30 No. 5,214,703,

grouping means which group said decrypted interblock and said transformer block, generating plaintext block,

output supplying means which supply multitude said plaintext block making up plaintext sequence,

whereby said plaintext sequence corresponds to said randomized-encrypted text sequence received by said first input means.

27. The system of claim 23 or 24 or 25 or 26 wherein said transformer block autonomous
5 generating means generate said transformer block implementing function H (said control initial block of length G).

28. The system of claim 27 wherein said grouping means include exclusive-OR operation.

10 29. The system of claim 28 wherein said transformer block autonomous generating means implement said function H (said control initial block of length G) for nth said transformer block as $H_n(R_i) = (H_{n-1}(R_i) \text{ oper } B) \bmod 2^{Q_i}$, wherein said Q_i less than or equal to 64, said R_i of length said Q_i is subblock of said control initial block of length G, said oper arithmetic operation selected from the group consisting of addition and subtraction and shift, said B value, said mod
15 module operation.

30. The system of claim 29 wherein said control initial block of length 2N made up preferably of 128 bits and said control initial block of length G made up preferably of 64 bits.

20 31. The system of claim 28 wherein said transformer block autonomous generating means implement said function H (said control initial block of length G) including random number generator.

32. The system of claim 31 wherein said control initial block of length 2N made up
25 preferably of 128 bits and said control initial block of length G made up preferably of seed length of said random number generator.

33. The system of claim 28 wherein said transformer block autonomous generating means implement said function H (said control initial block of length G) including hash function.

30 34. The system of claim 33 wherein said control initial block of length 2N made up preferably of 128 bits and said control initial block of length G made up preferably of zero or more bits.

PCT

PETITORIO

El abajo firmante pide que la presente solicitud internacional sea tramitada de conformidad con el Tratado de Cooperación en materia de Patentes.

Para uso de la Oficina receptora únicamente

Solicitud internacional N°

Fecha de presentación internacional

Nombre de la Oficina receptora y "Solicitud internacional PCT"

Referencia al expediente del solicitante o del mandatario (si se desea)
(como máximo, 12 caracteres)

Recuadro N° I TITULO DE LA INVENCION

SISTEMA DE ALEATORIZACION-ENCRIPTACION

Recuadro N° II SOLICITANTE

Nombre y dirección: (Apellido seguido del nombre; en el caso de una persona jurídica, la designación oficial completa. En la dirección deben figurar el código postal y el nombre del país. El país de la dirección indicada en este recuadro es el Estado de domicilio del solicitante si no se indica más abajo el Estado de domicilio.)

FERRE HERRERO, Angel José
Avgda. Constitució, 3 bis, 3º
43540 Sant Carles de la Rápita, Tarragona
ESPAÑA

☒ Esta persona es también un inventor.

N° de teléfono

(+34) 977740661

N° de facsimil

N° de teleimpresora

Estado de nacionalidad:

ES

Estado de domicilio:

ES

Esta persona es
solicitante para:



todos los Estados
designados



todos los Estados designados salvo
los Estados Unidos de América



los Estados Unidos de
América únicamente



los Estados indicados en el
recuadro suplementario

Recuadro N° III OTRO(S) SOLICITANTE(S) Y/O (OTRO(S)) INVENTOR(ES)

Nombre y dirección: (Apellido seguido del nombre; en el caso de una persona jurídica, la designación oficial completa. En la dirección deben figurar el código postal y el nombre del país. El país de la dirección indicada en este recuadro es el Estado de domicilio del solicitante si no se indica más abajo el Estado de domicilio.)

Esta persona es:

☐ solicitante únicamente

☐ solicitante e inventor

☐ inventor únicamente
(Si se marca esta casilla, no
se debe rellenar lo que sigue.)

Estado de nacionalidad:

Estado de domicilio:

Esta persona es
solicitante para:



todos los Estados
designados



todos los Estados designados salvo
los Estados Unidos de América



los Estados Unidos de
América únicamente



los Estados indicados en el
recuadro suplementario

☐ Los demás solicitantes y/o (demás) inventores se indican en una hoja de continuación.

Recuadro N° IV MANDATARIO O REPRESENTANTE COMUN; O DIRECCION PARA LA CORRESPONDENCIA

La persona abajo identificada se designa/ha sido designada para actuar en nombre del/
de los solicitante(s) ante las administraciones internacionales competentes como: ☐ mandatario ☐ representante común

Nombre y dirección: (Apellido seguido del nombre; en el caso de una persona jurídica, la designación oficial completa. En la dirección deben figurar el código postal y el nombre del país.)

N° de teléfono

N° de facsimil

N° de teleimpresora

☐ Dirección para la correspondencia: Márquese esta casilla cuando no se designe/se haya designado ningún mandatario o representante común y el espacio de arriba se utilice en su lugar para indicar una dirección especial a la que deba enviarse la correspondencia.

Recuadro N° V DESIGNACIONES DE ESTADOS

A continuación se hacen las designaciones siguientes en virtud de la Regla 4.9.a) (márquense las casillas adecuadas; debe marcarse por lo menos una):

Patente regional

- ☒ **AP** Patente ARIPO: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, SD Sudán, SZ Swazilandia, UG Uganda, ZW Zimbabwe, y cualquier otro Estado contratante del Protocolo de Harare y del PCT
- ☒ **EA** Patente Euroasiática: AM Armenia, AZ Azerbaiyán, BY Belarús, KG Kirguistán, KZ Kazakstán, MD República de Moldova, RU Federación de Rusia, TJ Tayikistán, TM Turkmenistán, y cualquier otro Estado contratante del Convenio sobre la Patente Euroasiática y del PCT
- ☒ **EP** Patente Europea: AT Austria, BE Bélgica, CH y LI Suiza y Liechtenstein, CY Chipre, DE Alemania, DK Dinamarca, ES España, FI Finlandia, FR Francia, GB Reino Unido, GR Grecia, IE Irlanda, IT Italia, LU Luxemburgo, MC Mónaco, NL Países Bajos, PT Portugal, SE Suecia, y cualquier otro Estado contratante del Convenio sobre la Patente Europea y del PCT
- ☒ **OA** Patente OAPI: BF Burkina Faso, BJ Benin, CF República Centroafricana, CG Congo, CI Côte d'Ivoire, CM Camerún, GA Gabón, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Níger, SN Senegal, TD Chad, TG Togo, y cualquier otro Estado que sea Estado miembro de la OAPI y que sea un Estado contratante del PCT (si se desea otra forma de protección o de tramitación, especifíquese en la línea de puntos)

Patente nacional (si se desea otra forma de protección o de tramitación, especifíquese en la línea de puntos):

- | | |
|--|---|
| <input checked="" type="checkbox"/> AL Albania | <input checked="" type="checkbox"/> LS Lesotho |
| <input checked="" type="checkbox"/> AM Armenia | <input checked="" type="checkbox"/> LT Lituania |
| <input checked="" type="checkbox"/> AT Austria | <input checked="" type="checkbox"/> LU Luxemburgo |
| <input checked="" type="checkbox"/> AU Australia | <input checked="" type="checkbox"/> LV Letonia |
| <input checked="" type="checkbox"/> AZ Azerbaiyán | <input checked="" type="checkbox"/> MD República de Moldova |
| <input checked="" type="checkbox"/> BA Bosnia y Herzegovina | <input checked="" type="checkbox"/> MG Madagascar |
| <input checked="" type="checkbox"/> BB Barbados | <input checked="" type="checkbox"/> MK Ex República Yugoslava de Macedonia |
| <input checked="" type="checkbox"/> BG Bulgaria | <input checked="" type="checkbox"/> MN Mongolia |
| <input checked="" type="checkbox"/> BR Brasil | <input checked="" type="checkbox"/> MW Malawi |
| <input checked="" type="checkbox"/> BY Belarús | <input checked="" type="checkbox"/> MX México |
| <input checked="" type="checkbox"/> CA Canadá | <input checked="" type="checkbox"/> NO Noruega |
| <input checked="" type="checkbox"/> CH y LI Suiza y Liechtenstein | <input checked="" type="checkbox"/> NZ Nueva Zelandia |
| <input checked="" type="checkbox"/> CN China | <input checked="" type="checkbox"/> PL Polonia |
| <input checked="" type="checkbox"/> CU Cuba | <input checked="" type="checkbox"/> PT Portugal |
| <input checked="" type="checkbox"/> CZ República Checa | <input checked="" type="checkbox"/> RO Rumania |
| <input checked="" type="checkbox"/> DE Alemania | <input checked="" type="checkbox"/> RU Federación de Rusia |
| <input checked="" type="checkbox"/> DK Dinamarca | <input checked="" type="checkbox"/> SD Sudán |
| <input checked="" type="checkbox"/> EE Estonia | <input checked="" type="checkbox"/> SE Suecia |
| <input checked="" type="checkbox"/> ES España | <input checked="" type="checkbox"/> SG Singapur |
| <input checked="" type="checkbox"/> FI Finlandia | <input checked="" type="checkbox"/> SI Eslovenia |
| <input checked="" type="checkbox"/> GB Reino Unido | <input checked="" type="checkbox"/> SK Eslovaquia |
| <input checked="" type="checkbox"/> GD Granada | <input checked="" type="checkbox"/> SL Sierra Leona |
| <input checked="" type="checkbox"/> GE Georgia | <input checked="" type="checkbox"/> TJ Tayikistán |
| <input checked="" type="checkbox"/> GH Ghana | <input checked="" type="checkbox"/> TM Turkmenistán |
| <input checked="" type="checkbox"/> GM Gambia | <input checked="" type="checkbox"/> TR Turquía |
| <input checked="" type="checkbox"/> HR Croacia | <input checked="" type="checkbox"/> TT Trinidad y Tabago |
| <input checked="" type="checkbox"/> HU Hungría | <input checked="" type="checkbox"/> UA Ucrania |
| <input checked="" type="checkbox"/> ID Indonesia | <input checked="" type="checkbox"/> UG Uganda |
| <input checked="" type="checkbox"/> IL Israel | <input checked="" type="checkbox"/> US Estados Unidos de América |
| <input checked="" type="checkbox"/> IN India | <input checked="" type="checkbox"/> UZ Uzbekistán |
| <input checked="" type="checkbox"/> IS Islandia | <input checked="" type="checkbox"/> VN Viet Nam |
| <input checked="" type="checkbox"/> JP Japón | <input checked="" type="checkbox"/> YU Yugoslavia |
| <input checked="" type="checkbox"/> KE Kenya | <input checked="" type="checkbox"/> ZW Zimbabwe |
| <input checked="" type="checkbox"/> KG Kirguistán | |
| <input checked="" type="checkbox"/> KP República Popular Democrática de Corea | |
| <input checked="" type="checkbox"/> KR República de Corea | |
| <input checked="" type="checkbox"/> KZ Kazakstán | |
| <input checked="" type="checkbox"/> LC Santa Lucía | |
| <input checked="" type="checkbox"/> LK Sri Lanka | |
| <input checked="" type="checkbox"/> LR Liberia | |

Casillas reservadas para designar Estados (a los fines de una patente nacional) que han pasado a formar parte del PCT después de la publicación de la presente hoja:

- ☒ **AE** Emiratos Árabes Unidos
- ☒ **ZA** Sudáfrica
- ☐

Declaración sobre la designación precautoria: Además de las designaciones arriba efectuadas, el solicitante efectuará también, en virtud de la Regla 4.9.b), todas las designaciones que estén permitidas con arreglo al PCT, salvo la designación o designaciones indicadas en el recuadro suplementario como excluido del ámbito de esta declaración. El solicitante declara que esas designaciones adicionales están sujetas a confirmación y que cualquier designación que no se confirme antes de que expiren los 15 meses a partir de la fecha prioritaria se considerará retirada por el solicitante al expirar dicho plazo. (La confirmación de una designación consiste en la presentación de un aviso en el que se especifique dicha designación, así como el pago de las tasas de designación y confirmación. La confirmación deberá llegar a la Oficina receptora dentro de ese plazo de 15 meses.)

Recuadro N° VI REIVINDICACION DE PRIORIDAD <input type="checkbox"/> Se indican otras reivindicaciones de prioridad en el recuadro suplementario.				
Fecha de presentación de la solicitud anterior (día/mes/año)	Número de la solicitud anterior	Si la solicitud anterior es:		
		solicitud nacional: país	solicitud regi. nal.* Oficina regi. nal	solicitud internacional: ficina receptora
Punto (1) 07 Mayo 1998 (07.05.98)	9801037	ES		
Punto (2) 22 Junio 1998 (22.06.98)	9801398	ES		
Punto (3)				

☒ Se ruega a la Oficina receptora que prepare y transmita a la Oficina Internacional una copia certificada de la solicitud anterior/de las solicitudes anteriores (sólo si la solicitud anterior ha sido presentada ante la oficina que a los fines de la presente solicitud internacional es la oficina receptora) identificada(s) supra como punto o puntos: (1) y (2)

* Si la solicitud anterior es una solicitud ARIPO, se indicará en el recuadro suplementario por lo menos a un Estado miembro del Convenio de París para la Protección de la Propiedad Industrial para el que ha sido presentada la solicitud anterior (Regla 4.10.b)ii). Véase el recuadro suplementario.

Recuadro N° VII ADMINISTRACION ENCARGADA DE LA BUSQUEDA INTERNACIONAL

Elección de la Administración encargada de la búsqueda internacional (Si dos o más Administraciones encargadas de la búsqueda internacional son competentes para efectuar la búsqueda internacional, indíquese el nombre de la Administración elegida; se puede utilizar el código de dos letras): **ISA / ES**

Petición para que se utilicen los resultados de la búsqueda anterior; referencia a esa búsqueda (si una búsqueda anterior ha sido realizada por o pedida a la Administración encargada de la búsqueda internacional):

Fecha (día/r. -/año): Número. País (u Oficina regional):

Recuadro N° VIII LISTA DE VERIFICACION; IDIOMA DE PRESENTACION

<p>La presente solicitud internacional contiene el siguiente número de hojas:</p> <p>petitorio : 3</p> <p>descripción (excepto la parte de la lista de secuencias) : 30</p> <p>reivindicaciones : 11</p> <p>resumen : 12</p> <p>dibujos : 12</p> <p>parte de la lista de secuencias de la descripción : 12</p> <p>Número total de hojas : 57</p>	<p>La presente solicitud internacional está acompañada de los documentos que se identifican a continuación:</p> <ol style="list-style-type: none"> <input checked="" type="checkbox"/> hoja de cálculo de tasas <input type="checkbox"/> poder separado firmado <input type="checkbox"/> copia del poder general; número de referencia, en su caso: <input type="checkbox"/> declaración que explica la ausencia de una firma <input type="checkbox"/> documento(s) de prioridad identificado(s) en el Recuadro N° VI como punto o puntos: <input type="checkbox"/> traducción de la solicitud internacional en (idioma): <input type="checkbox"/> indicación separada relativa a microorganismos depositados u otro material biológico <input type="checkbox"/> lista de secuencias de nucleótidos y/o aminoácidos en formato legible por ordenador <input type="checkbox"/> otros (especifíquese):
--	---

Figura de los dibujos que debe acompañar el resumen: 6

Idioma de presentación de la solicitud internacional: **ESPAÑOL**

Recuadro N° IX FIRMA DEL SOLICITANTE O DEL MANDATARIO

Junto a cada una de las firmas, indíquese el nombre de la persona que firma, así como su calidad (si dicha calidad no es evidente por lectura del petitorio).



Angel José FERRE HERRERO

Para la Oficina receptora únicamente	
1. Fecha efectiva de recepción de la pretendida solicitud internacional:	2. Dibujos: <input type="checkbox"/> recibidos: <input type="checkbox"/> no recibidos:
3. Fecha efectiva de recepción, rectificadas en razón de la recepción ulterior pero dentro del plazo, de documentos o de dibujos que completen la pretendida solicitud internacional:	
4. Fecha de recepción, dentro del plazo, de las correcciones solicitadas según el Artículo 11.2) del PCT:	
5. Administración de búsqueda internacional especificada por el solicitante: ISA /	6. <input type="checkbox"/> Transmisión de la copia para la búsqueda diferida hasta que se pague la tasa de búsqueda.

Para uso de la Oficina Internacional únicamente

Fecha de recepción del ejemplar original por la Oficina Internacional:

The demand must be filed directly with the competent International Preliminary Examining Authority. If two or more Authorities are competent, with the one chosen by the applicant. The name or two-letter code of that Authority may be indicated by the applicant on the line below:

IPEA/EP

PCT

CHAPTER II

DEMAND

under Article 31 of the Patent Cooperation Treaty:
The undersigned requests that the international application specified below be the subject of international preliminary examination according to the Patent Cooperation Treaty and hereby elects all eligible States (except where otherwise indicated).

For International Preliminary Examining Authority use only	
Identification of IPEA	Date of receipt of DEMAND
Box N . I IDENTIFICATION OF THE INTERNATIONAL APPLICATION	
International application No. PCT/ES99/00115	Applicant's or agent's file reference (Earliest) Priority date (day/month/year) 07 May 1998 (07.05.98)
International filing date (day/month/year) 30 April 1999 (30.04.99)	
Title of invention RANDOMIZATION-ENCRYPTION SYSTEM	
Box N . II APPLICANT(S)	
Name and address: (Family name followed by given name: for a legal entity, full official designation. The address must include postal code and name of country.) FERRE HERRERO, Angel José Avgda. Constitució, 3 bis, 3º 43540 Sant Carles de la Rápita, Tarragona ESPAÑA	Telephone No.: (+34) 977740661 Facsimile No.: (+34) 977740456 Teleprinter No.:
State (that is, country) of nationality: ES	State (that is, country) of residence: ES
Name and address: (Family name followed by given name: for a legal entity, full official designation. The address must include postal code and name of country.)	
State (that is, country) of nationality:	
State (that is, country) of residence:	
Name and address: (Family name followed by given name: for a legal entity, full official designation. The address must include postal code and name of country.)	
State (that is, country) of nationality:	
State (that is, country) of residence:	
<input type="checkbox"/> Further applicants are indicated on a continuation sheet.	

Box No. III AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCEThe following person is ☐ agent ☐ common representativeand ☐ has been appointed earlier and represents the applicant(s) also for international preliminary examination.☐ is hereby appointed and any earlier appointment of (an) agent(s)/common representative is hereby revoked.☐ is hereby appointed, specifically for the procedure before the International Preliminary Examining Authority, in addition to the agent(s)/common representative appointed earlier.Name and address: (Family name followed by given name: for a legal entity, full official designation.
The address must include postal code and name of country.)

Telephone No.:

Facsimile No.:

Teleprinter No.:

☐ Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.**Box No. IV BASIS FOR INTERNATIONAL PRELIMINARY EXAMINATION****Statement concerning amendments:***

1. The applicant wishes the international preliminary examination to start on the basis of:

☒ the international application as originally filed

the description

☐ as originally filed☐ as amended under Article 34

the claims

☐ as originally filed☐ as amended under Article 19 (together with any accompanying statement)☐ as amended under Article 34

the drawings

☐ as originally filed☐ as amended under Article 342. ☐ The applicant wishes any amendment to the claims under Article 19 to be considered as reversed.3. ☐ The applicant wishes the start of the international preliminary examination to be postponed until the expiration of 20 months from the priority date unless the International Preliminary Examining Authority receives a copy of any amendments made under Article 19 or a notice from the applicant that he does not wish to make such amendments (Rule 69.1(d)). (This check-box may be marked only where the time limit under Article 19 has not yet expired.)

* Where no check-box is marked, international preliminary examination will start on the basis of the international application as originally filed or, where a copy of amendments to the claims under Article 19 and/or amendments of the international application under Article 34 are received by the International Preliminary Examining Authority before it has begun to draw up a written opinion or the international preliminary examination report, as so amended.

Language for the purposes of international preliminary examination: ENGLISH☐ which is the language in which the international application was filed.☐ which is the language of a translation furnished for the purposes of international search.☐ which is the language of publication of the international application.☒ which is the language of the translation (to be) furnished for the purposes of international preliminary examination.**Box No. V ELECTION OF STATES**

The applicant hereby elects all eligible States (that is, all States which have been designated and which are bound by Chapter II of the PCT)

excluding the following States which the applicant wishes not to elect:

Box N . VI CHECK LIST

The demand is accompanied by the following elements, in the language referred to in Box No. IV, for the purposes of international preliminary examination:

- | | | |
|--|---|------------|
| 1. translation of international application | : | sheets |
| 2. amendments under Article 34 | : | sheets |
| 3. copy (or, where required, translation) of amendments under Article 19 | : | sheets |
| 4. copy (or, where required, translation) of statement under Article 19 | : | sheets |
| 5. letter | : | 1 sheets |
| 6. other (specify) | : | 5 4 sheets |

For International Preliminary Examining Authority use only

received not received

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

INTERNATIONAL APPLICATION AS FILED

The demand is also accompanied by the item(s) marked below:

- | | |
|--|---|
| 1. <input checked="" type="checkbox"/> fee calculation sheet | 4. <input type="checkbox"/> statement explaining lack of signature |
| 2. <input type="checkbox"/> separate signed power of attorney | 5. <input type="checkbox"/> nucleotide and or amino acid sequence listing in computer readable form |
| 3. <input type="checkbox"/> copy of general power of attorney; reference number, if any: | 6. <input type="checkbox"/> other (specify): |

Box No. VII SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE

Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the demand).



Angel José FERRE HERRERO

For International Preliminary Examining Authority use only

1. Date of actual receipt of DEMAND:

2. Adjusted date of receipt of demand due to CORRECTIONS under Rule 60.1(b):

3. ☐ The date of receipt of the demand is AFTER the expiration of 19 months from the priority date and item 4 or 5, below, does not apply.

☐ The applicant has been informed accordingly.

4. ☐ The date of receipt of the demand is WITHIN the period of 19 months from the priority date as extended by virtue of Rule 80.5.

5. ☐ Although the date of receipt of the demand is after the expiration of 19 months from the priority date, the delay in arrival is EXCUSED pursuant to Rule 82.

For International Bureau use only

Demand received from IPEA on:

PCT ORGANIZACION MUNDIAL DE LA PROPIEDAD INTELECTUAL
 Oficina Internacional
**SOLICITUD INTERNACIONAL PUBLICADA EN VIRTUD DEL TRATADO DE COOPERACION
 EN MATERIA DE PATENTES (PCT)**



(51) Clasificación Internacional de Patentes ⁶ : H04L 9/20, 9/28	A1	(11) Número de publicación internacional: WO 99/57845 (43) Fecha de publicación internacional: 11 de Noviembre de 1999 (11.11.99)
<div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> (21) Solicitud internacional: PCT/ES99/00115 (22) Fecha de la presentación internacional: 30 de Abril de 1999 (30.04.99) (30) Datos relativos a la prioridad: P 9801037 7 de Mayo de 1998 (07.05.98) ES P 9801398 22 de Junio de 1998 (22.06.98) ES (71)(72) Solicitante e inventor: FERRE HERRERO, Angel José [ES/ES]; Avenida Constitució, 3 bis, 3º, E-43540 Sant Carles de la Rapita (ES). </div> <div style="width: 48%;"> (81) Estados designados: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, Patente ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), Patente europea (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), Patente OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). </div> </div>		

Publicada

*Con informe de búsqueda internacional.
 Antes de la expiración del plazo previsto para la modificación de las reivindicaciones, será publicada nuevamente si se reciben modificaciones.*

(54) Title: RANDOMIZATION-ENCRYPTION SYSTEM

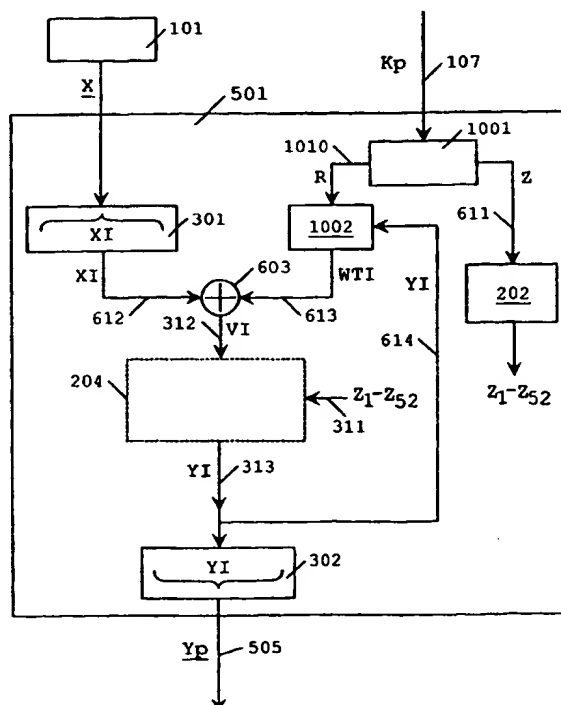
(54) Título: SISTEMA DE ALEATORIZACION-ENCRIPCIÓN

(57) Abstract

System for randomization-encryption of a sequence of data such that once provided the sequence of data (X) and the randomization-encryption key (Kp), the system generates a random data sequence (Yp) of which the confusion and diffusion can be measured objectively with the particular randomization-encryption key used (Kp). The data sequence (X) is divided into blocks (XI), each block (XI) being grouped with a transformer block (WTI) generated by a transformer block generator (1002) by using the initial control block (R) and of the anterior out block (YI); the grouped block (VI), which is the result of the grouping is encrypted with the device object of the patent US n° 5.214.703 (204), generating an out block (YI) which is provided to a transformer block generator (1002); the succession of out blocks (YI) forms the out randomized-encrypted sequence (Yp).

(57) Resumen

Sistema de aleatorización-encryptación de secuencia de datos tal que suministradas secuencia de datos (X) y clave de aleatorización-encryptación (Kp), genera secuencia de datos aleatoria (Yp), tal que legos en encryptación pueden medir objetivamente la confusión y difusión de la secuencia generada (Yp) con la particular clave de aleatorización-encryptación utilizada (Kp). La secuencia de datos (X) es dividida en bloques (XI), cada bloque (XI) se agrupa con bloque transformador (WTI), generado por generador de bloque transformador (1002) haciendo uso de bloque inicial de control (R) y de anterior bloque de salida (YI), dando el bloque agrupado (VI), resultado de la agrupación, que es encryptado con el dispositivo objeto de patente US n° 5.214.703 (204), generando un bloque de salida (YI) que es suministrado a generador de bloque transformador (1002), la sucesión de bloques de salida (YI) forma la secuencia aleatorizada-encryptada (Yp) de salida.



UNICAMENTE PARA INFORMACION

Códigos utilizados para identificar a los Estados parte en el PCT en las páginas de portada de los folletos en los cuales se publican las solicitudes internacionales en el marco del PCT.

AL	Albania	ES	España	LS	Lesotho	SI	Eslovenia
AM	Armenia	FI	Finlandia	LT	Lituania	SK	Eslovaquia
AT	Austria	FR	Francia	LU	Luxemburgo	SN	Senegal
AU	Australia	GA	Gabón	LV	Letonia	SZ	Swazilandia
AZ	Azerbaiyán	GB	Reino Unido	MC	Mónaco	TD	Chad
BA	Bosnia y Herzegovina	GE	Georgia	MD	República de Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tayikistán
BE	Bélgica	GN	Guinea	MK	Ex República Yugoslava de Macedonia	TM	Turkmenistán
BF	Burkina Faso	GR	Grecia	ML	Malí	TR	Turquía
BG	Bulgaria	HU	Hungría	MN	Mongolia	TT	Trinidad y Tabago
BJ	Benin	IE	Irlanda	MR	Mauritania	UA	Ucrania
BR	Brasil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarús	IS	Islandia	MX	México	US	Estados Unidos de América
CA	Canadá	IT	Italia	NE	Níger	UZ	Uzbekistán
CF	República Centroafricana	JP	Japón	NL	Países Bajos	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Noruega	YU	Yugoslavia
CH	Suiza	KG	Kirguistán	NZ	Nueva Zelandia	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	República Popular Democrática de Corea	PL	Polonia		
CN	Camerún	KR	República de Corea	PT	Portugal		
CU	Cuba	KZ	Kazakstán	RO	Rumania		
CZ	República Checa	LC	Santa Lucía	RU	Federación de Rusia		
DE	Alemania	LI	Liechtenstein	SD	Sudán		
DK	Dinamarca	LK	Sri Lanka	SE	Suecia		
EE	Estonia	LR	Liberia	SG	Singapur		

SISTEMA DE ALEATORIZACION-ENCRIPTACION

CAMPO TECNICO

5 La presente invención según se expresa en el título de la memoria descriptiva, se refiere a un sistema de aleatorización-encryptación de secuencia de datos digitales con una clave seleccionable libremente, en que la secuencia de datos encryptados es substancialmente aleatoria, con el correspondiente dispositivo recuperador de la mencionada secuencia de datos digitales a partir de la secuencia aleatorizada-encryptada haciendo uso de la clave seleccionable con la cual
10 se ha aleatorizado-encryptado.

La presente invención es especialmente aplicable en comunicaciones secretas, mantenimiento de la confidencialidad de la información, transacciones de comercio electrónico, comunicaciones por correo electrónico y semejantes.

15 ESTADO DE LA TECNICA

Como es conocido en el arte de la criptología, técnicas de encryptación (codificación) son usadas de modo que datos que están sujetos a vistas indeseadas, acostumbran a ser encryptados de tal forma que es difícil para uno que no esté autorizado a verlos, o usarlos, el que sea capaz
20 de hacerlo.

Como se acostumbra en el arte de la encryptación, el término "texto claro" se refiere a texto que no ha sido codificado o encryptado y acostumbra a ser directamente legible, y el término "texto cifrado" o "texto encryptado" se utiliza para referirse a texto que ha sido codificado, encryptado. También, los expertos en el arte reconocerán que, no obstante el nombre,
25 "texto claro" tiene la intención de incluir, no solo datos textuales, sino también datos binarios, tanto en la forma de fichero, por ejemplo un fichero de ordenador, o en la forma de datos en serie que son transmitidos, por ejemplo, desde un sistema de comunicación, como en un sistema de satélites, un sistema telefónico, o un sistema de correo electrónico entre otros.

Como es bien sabido por aquellos con conocimientos en el arte, hasta el momento un
30 número amplio de esquemas de encryptación han sido usados. Hasta el momento actual con los dispositivos de encryptación, entre los que se encuentran por mencionar algunos, como son, el dispositivo de encryptación "Data Encryption Standard" ("DES") del "American National Bureau of Standards", actual "National Institute of Standards and Technology" ("NBS" o "NIST") de Estados Unidos, el dispositivo de encryptación "Fast data encipherment algorithm

FEAL” (FEAL) desarrollado en Japón posteriormente, IECEJ Technical Report IT 86-33 (1986) y objeto de la patente US nº4,850,019 de título “Data Randomization Equipment”, el dispositivo de encriptación objeto de la patente US nº5,214,703 de título “Device for the conversion of a digital block and use of same”, así como el dispositivo de encriptación objeto de la patente US
5 nº5,675,653 de título “Method and apparatus for digital encryption”, el elemento o usuario que hace uso de ellos tras llevar a cabo la encriptación o cifrado de un texto claro siempre ha delegado la fortaleza de la invulnerabilidad de la encriptación ante ataques enemigos por descubrir el contenido del texto encriptado o la clave de encriptación con la que ha sido cifrado, en la confianza que ha de dar a organismos, instituciones o expertos que avalan la seguridad, así
10 como la confusión y difusión de valores que introduce el dispositivo de encriptación utilizado en el texto encriptado. El usuario o elemento que realiza la encriptación, de un texto claro en particular, no tiene una seguridad objetivable de la confusión y difusión de valores presente en el texto cifrado resultado de la aplicación del dispositivo de encriptación.

Anteriormente se ha aducido una aleatorización de un bloque de datos de entrada como es
15 el caso del dispositivo objeto de la patente US nº4,850,019 de título “Data randomization equipment”, cuyos inventores son Yokosuka Akihiro Shimizu y Yokohama Shoji Miyaguchi, ambos de Japón, en que se presentan dos encriptadores. En ambos casos la aleatorización de datos a la que se refieren es respecto al bloque individual de 64 bits que se da como datos de entrada, como se describe en la descripción de la patente en que está explicitado que “Datos
20 finales obtenidos del canal después de las operaciones funcionales y transformadoras son combinados por medios combinatorios para producir datos aleatorizados correspondientes a los datos de entrada”. Se puede además mencionar que la referida invención hace uso como clave de encriptación, en el primero de los encriptadores, de 64 bits de datos de clave, y en el segundo de los encriptadores hace uso como clave de encriptación de 128 bits de datos de clave.

25 El dispositivo de encriptación objeto de la patente US nº5,214,703 de título “Device for the conversion of a digital block and use of same”, de los inventores James L. Massey y Xuejia Lai, ambos de Suiza, es otro encriptador en que también el mensaje de texto encriptado resultado de su aplicación no presenta propiedades tales que hagan mensurables objetivamente, por parte del usuario o elemento que hace uso del dispositivo, la confusión y difusión de valores
30 que presenta el mencionado mensaje de texto encriptado y, al igual que el anterior dispositivo referenciado, la confusión y difusión introducidas son referentes al bloque de 64 bits de datos suministrado como entrada para ser encriptado. Se hace mención en la descripción de la mencionada patente que “puede ser probado de que la cantidad de cuatro operaciones es un mínimo para alcanzar el objetivo de difusión”, y por lo tanto, también relegando en expertos,

organismos o instituciones, el valorar la difusión y confusión que son introducidos en el texto encriptado resultado de su aplicación. Dicho dispositivo hace uso como clave de encriptación de 128 bits de datos de clave.

Otro ejemplo de dispositivo de encriptación en que se aduce una buena mezcla en el texto encriptado resultado es el dispositivo objeto de la patente US nº5,675,653 de título “Method and apparatus for digital encryption”, cuyo inventor es Nelson Douglas Valmore, Jr. En la mencionada patente se hace referencia también al hecho de que los expertos, las personas con conocimientos en el arte de la encriptación, reconocerán que las técnicas típicas de encriptación digital generalmente utilizan dos bien conocidas técnicas como son substitución y transposición; pero igualmente el dispositivo no presenta como resultado un texto encriptado tal que sea factible verificar objetivamente por legos en la materia la mezcla conseguida en el texto encriptado resultado.

También cabe decir que respecto a la clave de encriptación que se usa para llevar a cabo la encriptación, hasta este momento, existen recomendaciones sobre como debe ser la misma. Dichas recomendaciones son del tipo de las que se pueden encontrar en la publicación Federal Information Processing Standards Publication 112 o FIPS PUB 112, que anuncia el standard “Password usage”, del 30 de Mayo de 1985, del “National Institute of Standards and Technology” (“NIST”) del Departamento de Comercio del Gobierno de los Estados Unidos. Las mencionadas recomendaciones son referentes a longitud del “password” o “palabra de paso”, caracteres con los que es mejor que esté compuesta la password, y diferentes limitaciones en la composición del password, entre otras. Los entendidos en el arte reconocerán que las passwords tienen relación con las claves de encriptación y muchas veces son usadas como tales, tal como se recomienda en la misma publicación FIPS PUB 112 en diferentes secciones, como en la sección 3.9.3 de título “Transmission” del capítulo 3 de título “Acceptable Basic Criteria”; otra referencia en el mismo sentido se puede encontrar en la sección 3.7 de título “Storage” del capítulo 3 de título “Factors” del Apéndice A de título “Password Usage Guidelines” y en otros puntos del mencionado documento.

La clave de encriptación es elemento base transformador del texto claro en la encriptación del texto claro, puesto que son la combinación de las operaciones, más las propias operaciones que realiza el encriptador con el texto claro y la clave de encriptación lo que nos da el texto encriptado. La clave de encriptación utilizada es elemento transformador, diferenciador y variable de la serie de transformaciones que sufre el texto claro para producir el texto encriptado resultado. La clave de encriptación tiene influencia en la confusión y difusión que presenta el texto encriptado, por lo que de entre todas las claves que se pueden utilizar, existen unas que

introducirán más confusión y difusión de valores en el texto encriptado resultado que otras. Hasta el momento no se ha presentado un sistema de encriptación que pueda dar, como texto encriptado resultado de su aplicación, un texto tal que exista una manera medible y objetiva de discernir entre claves de encriptación que se pueden usar, cual o cuales producen mayor
5 difusión y confusión en los textos encriptados resultado con cada una de ellas.

Por lo tanto, se puede indicar que hasta el momento se ha dado el mismo valor de invulnerabilidad de un texto encriptado, resultado de la aplicación de un sistema de encriptación, a cualquier texto encriptado con cualquier clave de encriptación basándose en la opinión de expertos en cuanto a la difusión y confusión que introducen los sistemas de encriptación
10 utilizados. Los dispositivos de encriptación hasta el momento no dan como resultado un texto encriptado que presente substancialmente propiedades que permitan realizar una medición objetiva de la confusión y difusión que presenta.

Cada vez es más amplia la utilización de los dispositivos de encriptación por parte de legos en el arte de la encriptación, como ocurre por ejemplo con las transacciones comerciales
15 electrónicas, o el correo electrónico entre otros, en los que aquellas personas legos en el arte de la encriptación necesitan poder tener por ellos mismos una medida objetiva de la confusión y difusión presente en los datos encriptados. El poder disponer de un sistema de encriptación que de como resultado un texto encriptado tal que se pueda tener una medida objetiva de la confusión y difusión de valores, permitiría que legos en el arte de la encriptación puedan tener
20 una mayor seguridad en la confidencialidad de la información encriptada y por lo tanto usar con más confianza los sistemas de encriptación; esto ayudaría a que tengan una mayor aceptación y a un consiguiente incremento de uso, potenciándose internacionalmente con ello las comunicaciones de datos, correo electrónico y transacciones comerciales electrónicas entre otros.

Así mismo, respecto a la clave de encriptación no existe la posibilidad de discernir cual introduce más confusión y difusión, dando más confianza, en el texto cifrado debido a la no existencia de un sistema de encriptación cuyo texto encriptado presente substancialmente unas propiedades tales en que la confusión y difusión sean medibles objetivamente y por lo tanto permita discriminar entre diferentes claves de encriptación, que se pueden probar, cuales
30 producen un texto encriptado resultado en que esté presente una mayor difusión y confusión de valores.

Como se ha mencionado anteriormente aquellos entendidos en el arte de la encriptación reconocerán que es propósito de los dispositivos de encriptación introducir en el texto claro que se desea encriptar suficiente difusión y confusión de modo que no sea factible deducir a partir

del texto cifrado resultado el texto claro objeto de la encriptación o la clave de encriptación utilizada para realizar la encriptación. Así mismo, aquellos con conocimientos en el arte de los generadores de secuencias de números aleatorios, arte muy relacionado con el arte de la encriptación, reconocerán que en las secuencias de números aleatorios se da el mayor grado de difusión y confusión de valores. Para poder evaluar dichas secuencias de números aleatorios numerosos tests existen, como los descritos en “The Art of Computer Programming – 2ª Edición” Volumen 2 “Seminumerical Algorithms”, autor Donald E. Knuth, Addison-Wesley Publishing Company, ISBN: 0-201-03822-6(v.2) en las páginas 54 a 65; o los tests obligatorios descritos en el Federal Information Processing Standards Publication 140-1 o FIPS PUB 140-1, de título “Security requirements for cryptographic modules”, del 11 de Enero de 1994, del “National Institute of Standards and Technology” (“NIST”) del Departamento de Comercio del Gobierno de los Estados Unidos, en la sección 4.11.1 de título “Power-Up Tests”, tests a que deben ser sometidos los generadores de secuencias de números aleatorios. Aunque como se describe en la anteriormente mencionada publicación “The Art of Computer Programming – 2ª Edición” Volumen 2 “Seminumerical Algorithms” autor Donald E. Knuth, Addison-Wesley Publishing Company ISBN: 0-201-03822-6(v.2) en la página 35 líneas 13 a 18, el hecho de que una secuencia se comporte aleatoriamente con respecto a tests T_1, T_2, \dots, T_n , no permite asegurar que no falle al aplicarla al test T_{n+1} ; pero cada test de aleatoriedad aplicado dará más y más confianza en la aleatoriedad de la secuencia y por lo tanto en la confusión y difusión de valores presente.

El hecho de disponer de un sistema de encriptación tal que el texto encriptado resultado de su utilización presentase substancialmente las propiedades de las secuencias de números aleatorios permitiría aplicar de un modo computacionalmente factible tests de aleatoriedad, como los anteriormente mencionados, al texto encriptado resultado y por lo tanto tener una medida objetiva de la difusión y confusión presentes en cada texto encriptado. Los legos en el arte de la encriptación podrían tener, para cada texto encriptado por ellos mismos, una medida objetiva de la difusión y confusión presentes en el texto encriptado, lo que les infundiría más confianza en la confidencialidad de la información. Además si se da el caso de que una clave de encriptación utilizada con una secuencia de texto claro, no generase lo que se pudiese considerar suficiente difusión y confusión en el texto aleatorizado-encriptado resultado, sin demérito de las recomendaciones usuales referentes a claves de encriptación como las comentadas anteriormente, podría someterse al texto claro a un nuevo proceso de encriptación, con una clave de encriptación diferente, hasta que la confusión y difusión logradas fuesen las deseadas.

EXPLICACION DE LA INVENCION

La presente invención es un sistema para la aleatorización-encryptación de texto claro que va a ser transmitido a través de un medio, por un canal de transmisión o comunicaciones por ejemplo, en el cual puede ser visto, analizado o interceptado. Por ejemplo, y sin limitar lo precedente, un canal de transmisión o comunicación puede incluir una red de ordenadores, líneas de sistemas telefónicos terrestres, o celulares, una transmisión vía satélite, un disco de ordenador, y cualquier otro tipo de medio que pueda ser utilizado para la transferencia de datos en forma digital. Como se utiliza aquí, "canal de transmisión" simplemente significa el medio sobre el que datos digitales son transportados.

En vista de las cuestiones que plantea el actual estado de la técnica, el objeto de la presente invención es suministrar un sistema de encryptación de datos tal que la secuencia de datos de salida no solo esté encryptada o cifrada, sino que esté aleatorizada de tal modo que permite evaluar la confusión y difusión que presenta la secuencia de datos encryptados de salida; y por lo tanto poder seleccionar la clave de encryptación utilizada al disponerse de una medida objetiva de la confusión y difusión de valores que la misma introduce en el texto aleatorizado-encryptado.

Aunque la técnica que se entiende como cifrador de flujos, descrita en las páginas 589 a 592 del libro "Redes de ordenadores" Segunda Edición, autor Andrew S. Tanenbaum, editado por "Prentice-Hall Hispanoamericana, S.A.", ISBN: 968-880-176-3, y otros modos similares, como los descritos en la publicación Federal Information Processing Standards Publication 81 o FIPS PUB 81, que anuncia el standard "DES Modes of Operation", del "National Institute of Standards and Technology" ("NIST") del Departamento de Comercio del Gobierno de los Estados Unidos, son hace tiempo utilizados en el arte de la encryptación, por sí mismos no generan secuencias substancialmente aleatorias a las cuales les fuese computacionalmente factible la aplicación de tests de aleatoriedad como los anteriormente referenciados.

El sistema de la presente invención consigue los propósitos de generación de secuencias de datos encryptados substancialmente aleatorizadas haciendo uso del encryptador de bloques objeto de la patente US nº5,214,703 de título "Device for the conversion of a digital block and use of same"; permitiendo además hacer uso de una clave de encryptación de longitud más larga en función de la realización específica de la invención.

De acuerdo a la invención, el dispositivo de aleatorización-encryptación consta de medios para recibir por primera entrada secuencia de datos y de medios para recibir por segunda entrada bloque de control. Mencionado bloque de control por medios divisores de bloque de control es

dividido en dos bloques iniciales de control, bloque inicial de control de longitud G y bloque inicial de control de longitud 2N. Medios generadores de subbloques de control de encriptación con mencionado bloque inicial de control de longitud 2N generan subbloques de control de encriptación de longitud M. Medios generadores de bloque transformador con mencionado
5 bloque inicial de control de longitud G, y con bloque de salida de longitud N cuando es suministrado, generan multitud de bloques transformador. Medios ensambladores ensamblan bloques de datos de longitud N de mencionada secuencia de datos. Medios agrupadores agrupan correspondiente mencionado bloque transformador y correspondiente mencionado bloque de datos de longitud N dando un interbloque de longitud N. Mencionado interbloque de longitud N
10 se suministra como entrada de encriptador objeto de la patente US nº5,214,703, donde es agrupado con mencionados subbloques de control de encriptación de longitud M, dando bloque de salida de longitud N. Mencionado bloque de salida de longitud N se suministra como salida del dispositivo de aleatorización-encriptación objeto de la presente invención y también se suministra a mencionados medios generadores de bloque transformador que generan
15 correspondiente nuevo bloque transformador para la aleatorización-encriptación del correspondiente siguiente bloque de datos de longitud N. Medios de salida son proporcionados para transmitir la secuencia de datos aleatorizada-encriptada formada por los bloques de salida de longitud N.

El dispositivo integrante de la invención para la recuperación de la secuencia de datos
20 consta de medios para recibir por primera entrada secuencia de datos aleatorizada-encriptada y de medios para recibir por segunda entrada bloque de control. Mencionado bloque de control por medios divisores de bloque de control es dividido en dos bloques iniciales de control, bloque inicial de control de longitud G y bloque inicial de control de longitud 2N. Medios generadores de subbloques de control de desencriptación con mencionado bloque inicial de control de
25 longitud 2N generan subbloques de control de desencriptación de longitud M. Medios generadores de bloque transformador con mencionado bloque inicial de control de longitud G, y con bloque de datos aleatorizados-encriptados de longitud N cuando es suministrado, generan multitud de bloques transformador. Medios ensambladores ensamblan bloques de datos aleatorizados-encriptados de longitud N de mencionada secuencia de datos aleatorizada-
30 encriptada. Mencionado bloque de datos aleatorizados-encriptados de longitud N se suministra como entrada de encriptador objeto de patente US nº5,214,703, donde es agrupado con mencionados subbloques de control de desencriptación de longitud M, dando interbloque de longitud N. Medios agrupadores agrupan correspondiente mencionado bloque transformador y correspondiente mencionado interbloque de longitud N dando bloque de salida de longitud N.

Mencionado bloque de salida de longitud N se suministra como salida del dispositivo de descriptación de la presente invención. Mencionado bloque de datos aleatorizados-encryptados se suministra a mencionados medios generadores de bloque transformador que generan correspondiente nuevo bloque transformador para la descriptación del correspondiente
5 siguiente bloque de datos aleatorizados-encryptados de longitud N. Medios de salida son proporcionados para transmitir la secuencia de datos formada por los bloques de salida de longitud N, correspondientes a la secuencia de datos aleatorizados-encryptados.

Una primera variante del sistema de aleatorización-encryptación de la invención, respecto a la exposición previa, es tal que en ambos dispositivos el bloque de control está compuesto por
10 el bloque inicial de control de longitud $2N$ y es suministrado directamente a los medios generadores de subbloques de control de longitud M con la correspondiente eliminación de los medios divisores de bloque de control, estando el bloque inicial de control de longitud G suministrado a los medios generadores de bloque transformador prefijado en los dispositivos para la aleatorización-encryptación de la secuencia de texto claro o descriptación de la
15 secuencia de datos aleatorizados-encryptados. Presenta esta variante el inconveniente de hacer uso de un bloque de control de menor longitud.

De acuerdo a la invención, una tercera realización del aleatorizador-encryptador consta de medios para recibir por primera entrada secuencia de datos y de medios para recibir por segunda
20 entrada bloque de control. Mencionado bloque de control por medios divisores de bloque de control es dividido en dos bloques iniciales de control, bloque inicial de control de longitud G y bloque inicial de control de longitud $2N$. Medios generadores de subbloques de control de encryptación con mencionado bloque inicial de control de longitud $2N$ generan subbloques de control de encryptación de longitud M . Medios generadores autónomos de bloque transformador con mencionado bloque inicial de control de longitud G generan multitud de bloques
25 transformador. Medios ensambladores ensamblan bloques de datos de longitud N de mencionada secuencia de datos. Medios agrupadores agrupan correspondiente mencionado bloque transformador y correspondiente mencionado bloque de datos de longitud N dando un interbloque de longitud N . Mencionado interbloque de longitud N se suministra como entrada de dispositivo de encryptación objeto de patente US nº5,214,703, donde es agrupado con
30 mencionados subbloques de control de encryptación de longitud M , dando bloque de salida de longitud N . Mencionado bloque de salida de longitud N se suministra como salida del dispositivo de aleatorización-encryptación objeto de la presente invención. Medios de salida son proporcionados para transmitir la secuencia de datos aleatorizada-encryptada formada por los bloques de salida de longitud N .

El dispositivo integrante de la invención para la recuperación de la secuencia de datos aleatorizada-encryptada con la tercera realización del aleatorizador-encritpador consta de medios para recibir por primera entrada secuencia de datos aleatorizada-encryptada y de medios para recibir por segunda entrada bloque de control. Mencionado bloque de control por medios divisores de bloque de control es dividido en dos bloques iniciales de control, bloque inicial de control de longitud G y bloque inicial de control de longitud $2N$. Medios generadores de subbloques de control de descryptación con mencionado bloque inicial de control de longitud $2N$ generan subbloques de control de descryptación de longitud M . Medios generadores autónomos de bloque transformador con mencionado bloque inicial de control de longitud G generan multitud de bloques transformador. Medios ensambladores ensamblan bloques de datos aleatorizados-encryptados de longitud N de mencionada secuencia de datos aleatorizada-encryptada. Mencionado bloque de datos aleatorizados-encryptados de longitud N se suministra como entrada de dispositivo de encryptación objeto de patente US nº5,214,703, donde es agrupado con mencionados subbloques de control de descryptación de longitud M , dando interbloque de longitud N . Medios agrupadores agrupan correspondiente mencionado bloque transformador y correspondiente mencionado interbloque de longitud N dando bloque de salida de longitud N . Mencionado bloque de salida de longitud N se suministra como salida del dispositivo de descryptación de la presente invención. Medios de salida son proporcionados para transmitir la secuencia de datos formada por los bloques de salida de longitud N .

Una cuarta variante del dispositivo de encryptación de la invención, respecto a la exposición de la tercera realización, es tal que el bloque de control está compuesto por el bloque inicial de control de longitud $2N$ y es suministrado directamente a los respectivos medios generadores de subbloques de control de longitud M con la eliminación de los medios divisores de bloque de control, estando el bloque inicial de control de longitud G suministrado a los medios generadores autónomos de bloque transformador prefijado en el dispositivo para la aleatorización-encryptación de la secuencia de texto claro y descryptación de la secuencia de texto aleatorizado-encryptado.

A continuación para facilitar una mejor comprensión de esta memoria y formando parte integrante de la misma se acompaña una serie de figuras en las que con carácter ilustrativo y no limitativo se ha representado el objeto de la invención.

BREVE DESCRIPCION DE LAS FIGURAS

La Fig.1 muestra arte previo de diagrama básico de enlazado de bloques de un sistema

para la transmisión y tratamiento de datos en forma encriptada.

La Fig.2 muestra arte previo de diagrama de cableado de bloques de encriptador de bloque objeto de patente US nº5,214,703, mostrada para facilitar posteriores referencias de la presente invención.

5 La Fig.3 muestra arte previo de diagrama de cableado de bloques de encriptador de bloque objeto de patente US nº5,214,703, esquematizado con respecto al representado en la Fig.2, con elementos relevantes de la misma para la realización de la presente invención.

La Fig.4 muestra arte previo de diagrama de cableado de bloques de descryptador de bloque objeto de patente US nº5,214,703, esquematizado con respecto al representado en la Fig.2, con elementos relevantes de la misma para la realización de la presente invención.

La Fig.5 muestra diagrama básico de enlazado de bloques de un sistema para la transmisión de datos en forma aleatorizada-encriptada haciendo uso de los dispositivos de aleatorización-encriptación y descryptación objetos de la presente invención.

La Fig.6 muestra aleatorizador-encriptador para la aleatorización-encriptación de un mensaje de texto claro de acuerdo con la presente invención. En conjunción con la Fig.7 muestra el mejor modo de realización de la invención.

La Fig.7 muestra descryptador para la descryptación de secuencias aleatorizadas-encriptadas con dispositivo de la Fig.6.

La Fig.8 muestra segunda realización de aleatorizador-encriptador con las variaciones aplicadas con respecto al dispositivo de la Fig.6.

La Fig.9 muestra descryptador para la descryptación de secuencias de texto aleatorizadas-encriptadas con dispositivo de la Fig.8.

La Fig.10 muestra tercera realización de aleatorizador-encriptador con variaciones aplicadas con respecto al dispositivo de la Fig.6.

25 La Fig.11 muestra descryptador para la descryptación de secuencias aleatorizadas-encriptadas con dispositivo de la Fig.10.

La Fig.12 muestra cuarta realización de aleatorizador-encriptador con variaciones aplicadas con respecto al dispositivo de la Fig.10.

La Fig.13 muestra descryptador para la descryptación de secuencias aleatorizadas-encriptadas con dispositivo de la Fig.12.

MODOS DE REALIZACION DE LA INVENCION

La Fig.1 muestra arte previo de diagrama de sistema generalmente utilizado para la

transmisión y tratamiento de datos en forma encriptada. Los datos (secuencia de texto claro X) a ser transmitidos son originados en una fuente del mensaje 101, por ejemplo un ordenador, suministrándose a un encriptador 102 y son transmitidos como secuencia de texto encriptado Y por un canal de transmisión 103, llegando al descryptador 104 en el lado del receptor el cual alimenta al destino 105, por ejemplo un segundo ordenador, con la secuencia de texto claro X. Para la encriptación y descryptación de los datos, el encriptador 102 y el descryptador 104 usan un bloque de control o clave de encriptación Z, el cual se suministra desde una fuente de clave 106 por el canal 107 al encriptador 102 y por un canal seguro 108, que puede ser por ejemplo un correo con un cubrimiento sellado, al descryptador 104. La secuencia de texto encriptado Y en el canal de transmisión 103 está siempre expuesto al riesgo de que un criptoanálisis enemigo 109 con la secuencia de texto encriptado Y intentará obtener la secuencia de texto claro X o la clave de encriptación Z (los resultados de estos intentos están designados por $\sim X$ y $\sim Z$).

Hasta el momento la ocultación del contenido de la secuencia de texto claro X en la secuencia de texto encriptado Y reside en la avalada confusión y difusión introducida por el encriptador usado ante criptoanálisis enemigos 109, con independencia de la clave de encriptación Z usada.

La Fig.2 muestra diagrama de encriptador 102 de la Fig.1, objeto de patente US n°5,214,703 de título "Device for the conversion of a digital block and use of same", teniendo correspondencia con la Fig.2 de la mencionada patente, y mostrada para posteriores referencias. En la Fig.2 las referencias alfabéticas utilizadas son las mismas referencias alfabéticas que se usan en la mencionada Fig.2 y descripción de la patente US n°5,214,703, de modo que sea más sencillo conocer el objeto de las mismas, las referencias numéricas han sido modificadas con el objeto de adecuarlas a la presente memoria. El encriptador 102 encripta la secuencia de texto claro X dando la secuencia de texto encriptado Y haciendo uso de bloque de control Z que llega por canal 107. Durante el proceso de encriptación, los subbloques de control son subbloques de control de encriptación Z_1 a Z_{52} , mientras en el proceso de descryptación son subbloques de control de descryptación U_1 a U_{52} , los cuales son también derivados del bloque de control Z; el bloque de control Z será referido en la exposición de los modos de realización de la presente invención como bloque inicial de control Z, utilizándose la denominación bloque de control para designar la clave de aleatorización-encriptación de la presente invención. El método para la obtención de los subbloques de control de encriptación Z_1 a Z_{52} , del bloque de control Z por el generador de subbloques de control de encriptación 202 es descrito en mencionada patente US

nº5,214,703 haciendo uso de mismas referencias alfanuméricas.

El encriptador-desencriptador 204 necesario para el proceso de encriptación $X \rightarrow Y$ está indicado como línea discontinua en la Fig.2 y será referenciado de este modo posteriormente.

5 La Fig.3 muestra diagrama esquematizado de encriptador 102 de la Fig.2 con elementos relevantes para la descripción de la presente invención que serán referenciados posteriormente. En la Fig.3, partes correspondientes a partes de la Fig.2 son designadas por mismas referencias. La secuencia de texto claro X a ser cifrada llega continuamente de la fuente del mensaje 101 al ensamblador de entrada de bloque de longitud N 301, por ejemplo un convertidor serie/paralelo
10 en el caso de una fuente de bits serie, el cual ensambla bloques de texto claro de longitud N X de longitud preferentemente $N=64$ bits. Los subbloques de texto claro de longitud M X_1, X_2, X_3, X_4 de la Fig.2 juntos forman el bloque de texto claro de longitud N X mostrado en la Fig.3. Este bloque de texto claro de longitud N X llega al encriptador-desencriptador 204 por entrada 312. La entrada 312 es la agrupación de las cuatro entradas 210 a 213 de la Fig.2, formadas por 16
15 líneas paralelas cada una. Durante el proceso de encriptación, los bloques de control son subbloques de control de encriptación Z_1 a Z_{52} , de longitud $M=16$ bits cada uno, derivados del bloque de control Z recibido por canal 107 en el generador de subbloques de control de encriptación 202, que llegan al encriptador-desencriptador 204 por entrada 311. La entrada 311 representa la agrupación de las 52 entradas 240 a 291 del encriptador-desencriptador 204 de la
20 Fig.2. Un bloque de texto encriptado de longitud N Y, aparece en la salida 313 del encriptador-desencriptador 204. Los subbloques de texto encriptado de longitud M Y_1, Y_2, Y_3, Y_4 de la Fig.2 juntos forman el bloque de texto encriptado de longitud N Y mostrado en la Fig.3. La salida 313 es la agrupación de las cuatro salidas 230 a 233, de 16 líneas paralelas cada una, de la Fig.2. Este bloque de texto encriptado de longitud N Y es transmitido desde una unidad de
25 salida de bloque de longitud N 302, por ejemplo un convertidor paralelo/serie. La sucesión de bloques de texto encriptado de longitud N Y forman la secuencia de texto encriptado Y transmitida por el canal de transmisión 103.

La Fig.4 muestra diagrama de desencriptador 104, esquematizado con respecto al
30 representado en la Fig.2 de la presente, con elementos relevantes para la descripción de la presente invención que serán referenciados posteriormente. En la Fig.4, partes correspondientes a partes de la Fig.1, Fig.2 y Fig.3 son designadas por mismas referencias. La secuencia de texto encriptado Y llega al ensamblador de entrada de bloque de longitud N 301 que ensambla bloques de texto encriptado de longitud N Y de longitud preferentemente $N=64$ bits que llegan

al encriptador-desencriptador 204 por entrada 312. El bloque de texto encriptado de longitud N Y representa la agrupación de los cuatro subbloques de texto claro de longitud M X1, X2, X3, X4 de la Fig.2.

5 Durante el proceso de desencriptación, los bloques de control son subbloques de control de desencriptación U_1 a U_{52} , de longitud $M=16$ bits cada uno, derivados del bloque de control Z en el generador de subbloques de control de desencriptación 401 tal como se describe en la mencionada patente US nº5,214,703 haciendo uso de mismas referencias alfanuméricas. En el encriptador-desencriptador 204 se agrupan el bloque de texto encriptado de longitud N Y y los cincuenta y dos subbloques de control de desencriptación U_1 a U_{52} que llegan por entrada 311, dando un bloque de texto claro de longitud N X de longitud $N=64$ bits por salida 313. El bloque de texto claro de longitud N X representa la agrupación de los cuatro subbloques de texto encriptado de longitud M Y1, Y2, Y3, Y4 de la Fig.2. Este bloque de texto claro de longitud N X es transmitido desde una unidad de salida de bloque de longitud N 302 al destino 105. La sucesión de bloques de texto claro de longitud N X forman la secuencia de texto claro X.

15

La Fig.5 muestra posible diagrama de sistema para la transmisión de datos en forma aleatorizada-encriptada haciendo uso de los dispositivos de aleatorización-encriptación y desencriptación objeto de la presente invención. En la Fig.5, partes correspondientes a partes de la Fig.1 son designadas por mismas referencias. Los datos (secuencia de texto claro X) son originados en una fuente del mensaje 101, siendo aleatorizados-encriptados en aleatorizador-encriptador 501 haciendo uso de clave de aleatorización-encriptación K_p , en la presente memoria lo denominaremos bloque de control K_p , que se suministra desde una fuente de clave 504 por medio del canal 107, dando como resultado una secuencia de texto aleatorizado-encriptado candidata Yp. La secuencia de texto aleatorizado-encriptado candidata Yp, entre una de las múltiples configuraciones del sistema posibles, puede alcanzar por una línea de transmisión 505 a un emisor mensaje encriptado 506, a la espera del resultado de la aplicación de los tests de aleatoriedad en analizador de aleatoriedad 503.

25

Dadas las substanciales propiedades de las secuencias aleatorias que presenta la secuencia de texto aleatorizado-encriptado candidata Yp generada en el aleatorizador-encriptador 501 es sometible a un análisis de aleatoriedad en analizador de aleatoriedad 503 para tener conocimiento del cumplimiento de las mencionadas propiedades de las secuencias aleatorias y tener una medida objetiva de la confusión y difusión que presenta. El resultado de la aplicación a la secuencia de texto aleatorizado-encriptado candidata Yp de los tests de aleatoriedad en el analizador de aleatoriedad 503 es designado como resultado aleatoriedad T_p , del cual se informa

30

a la fuente de clave 504.

El mencionado analizador de aleatoriedad 503 puede ser una implementación hardware o software de una selección o la totalidad de diferentes tests de aleatoriedad existentes, como los descritos en “The Art of Computer Programming – 2ª Edición” Volumen 2 “Seminumerical Algorithms” autor Donald E. Knuth, Addison-Wesley Publishing Company, ISBN: 0-201-03822-6(v.2) en las páginas 54 a 65, o los tests obligatorios presentados en el Federal Information Processing Standards Publication 140-1 o FIPS PUB 140-1, de título “Security requirements for cryptographic modules”, del 11 de Enero de 1994, del “National Institute of Standards and Technology” (“NIST”) del Departamento de Comercio del Gobierno de los Estados Unidos, en la sección 4.11.1 de título “Power-Up Tests”, a que deben ser sometidos los generadores de secuencias de números aleatorios a ser utilizados en módulos criptográficos gubernamentales del citado país. Como se describe en la anteriormente mencionada publicación “The Art of Computer Programming – 2ª Edición” Volumen 2 “Seminumerical Algorithms”, autor Donald E. Knuth, Addison-Wesley Publishing Company ISBN: 0-201-03822-6(v.2) en la página 35, líneas 13 a 18, el hecho de que una secuencia se comporte aleatoriamente con respecto a los tests T_1, T_2, \dots, T_n , no puede asegurar que no falle al aplicarla al test T_{n+1} ; pero cada test de aleatoriedad aplicado dará más y más confianza en la aleatoriedad de la secuencia, y por lo tanto en la confusión y difusión de valores presente en la secuencia.

Con el resultado aleatoriedad T_p la fuente de clave 504 puede llevar a cabo dos acciones. Uno, puede decidir la transmisión de la secuencia de texto aleatorizado-encryptado candidata $\underline{Y_p}$ por el canal de transmisión 103 como secuencia de texto aleatorizado-encryptado $\underline{Y_s}$, representado por medio de la señal de envío S , y proveer el bloque de control K_p utilizado por medio del canal seguro 108 como bloque de control seleccionado K_s al descryptador 502. Dos, puede decidir seleccionar un nuevo bloque de control K_p , someter la secuencia de texto claro \underline{X} a nueva aleatorización-encryptación en aleatorizador-encryptador 501, y verificar la nueva secuencia de texto aleatorizado-encryptado candidata $\underline{Y_p}$ en el analizador de aleatoriedad 503.

La secuencia de texto aleatorizado-encryptado $\underline{Y_s}$, que es la secuencia de texto aleatorizado-encryptado candidata $\underline{Y_p}$ seleccionada que es transmitida, llega al descryptador 502, que alimenta al destino 105 con la secuencia de texto claro \underline{X} . Para la descryptación, el descryptador 502 usa el bloque de control seleccionado K_s que se suministra desde la fuente de clave 504 por medio del canal seguro 108.

La secuencia de texto aleatorizado-encryptado $\underline{Y_s}$ en el canal de transmisión 103 está siempre expuesta al riesgo de que un criptoanálisis enemigo 109 intentará obtener la secuencia texto claro \underline{X} o el bloque control seleccionado K_s (los resultados de estos intentos están

designados por $\sim X$ y $\sim K_s$).

En los dispositivos de encriptación existentes hasta el momento la confusión y difusión de valores que presenta la secuencia de texto encriptado Y transmitida por el canal de transmisión reside en la confusión y difusión avalada por expertos, instituciones u organismos que introduce el algoritmo de encriptación usado, con independencia de la clave de encriptación usada. Pero las secuencias de texto encriptado Y particulares resultado de su aplicación no presentan características tales que sea computacionalmente factible tener una medida objetiva de la confusión y difusión de los valores que componen la secuencia de texto encriptado Y . Con la presente invención el dispositivo de cifrado da como resultado de su aplicación texto cifrado tan substancialmente aleatorizado, que permite poder tener una medida objetiva de la confusión y difusión de valores presente en una secuencia de texto aleatorizado-encriptado Y_s particular resultado de una aleatorización-encriptación de una secuencia de texto claro X particular con un bloque de control seleccionado K_s particular; permitiendo diferenciar entre diferentes bloques de control K_p la difusión y confusión que generan en la secuencia de texto aleatorizado-encriptado candidata Y_p , y por lo tanto tener la posibilidad de elección de aquella que de más seguridad subjetiva en cuanto a la resistencia de la secuencia de texto aleatorizado-encriptado Y_s ante criptoanálisis enemigos.

La Fig.6 muestra posible diagrama de aleatorizador-encriptador para aleatorización-encriptación de secuencia de texto claro de acuerdo con la invención. En la Fig.6, partes correspondientes a partes de las Fig.1, Fig.3 y Fig.5 son designadas por mismas referencias.

El divisor de bloque de control 1001 por canal 107 recibe el bloque de control K_p , dividiéndolo en dos bloques iniciales de control, bloque inicial de control Z , de longitud preferentemente $L_1=128$ bits, y bloque inicial de control R , de longitud preferentemente $L_2=G$ bits. El bloque inicial de control Z por salida 611 se suministra al generador de subbloques de control de encriptación 202 que genera los subbloques de control de encriptación Z_1 a Z_{32} que son suministrados por entrada 311 al encriptador-desencriptador 204. El subbloque inicial de control R se suministra al generador de bloque transformador 1002 por salida 1010.

La secuencia de texto claro X a ser aleatorizada-encriptada llega continuamente de la fuente del mensaje 101 al ensamblador de entrada de bloque de longitud N 301, el cual ensambla bloques de texto claro X_i de longitud preferentemente $N=64$ bits de la secuencia de texto claro X siendo suministrados por salida 612 al agrupador 603. El agrupador 603 presenta entradas 612 y 613 y salida 312, de 64 líneas paralelas cada una; en el agrupador 603 se agrupan el correspondiente bloque de texto claro X_i y correspondiente bloque transformador WT_i ,

ambos de longitud $N=64$ bits que llegan por entradas 612 y 613 respectivamente, generando el correspondiente interbloque agrupado VI de longitud $N=64$ bits por salida 312. La operación de agrupación que se realiza en el agrupador 603 es la OR-exclusiva o XOR bit a bit, de tal modo que $XI \oplus WTI \rightarrow VI$.

5 Este interbloque agrupado VI por entrada 312 alcanza al encriptador-desencriptador 204 donde es agrupado junto con los cincuenta y dos subbloques de control de encriptación Z_1 a Z_{52} que llegan por entrada 311, dando un bloque de texto aleatorizado-encriptado YI de longitud $N=64$ bits, por salida 313. La salida 313, formada por 64 líneas paralelas, está conectada a la unidad de salida de bloque de longitud N 302 y por entrada 614, que tiene como posible
10 implementación ser derivación de salida 313, al generador de bloque transformador 1002. El bloque de texto aleatorizado-encriptado YI alcanza la unidad de salida de bloque de longitud N 302 y se suministra al generador de bloque transformador 1002 para ser utilizado en la generación por el generador de bloque transformador 1002 del correspondiente bloque transformador WTI a ser utilizado en la aleatorización-encriptación del siguiente bloque de texto
15 claro XI ensamblado en el ensamblador de entrada de bloque de longitud N 301. Este bloque de texto aleatorizado-encriptado YI puede ser convertido en una unidad de salida de bloque de longitud N 302 de tal forma que puede ser transmitido por la línea de transmisión 505. Los bloques de texto aleatorizado-encriptado YI juntos forman la secuencia de texto aleatorizado-encriptado candidata Y_p .

20 El propósito del generador de bloque transformador 1002, al igual que los respectivos generadores de bloque transformador de las Fig.8, Fig.10 y Fig.12 es suministrar el correspondiente bloque transformador WTI al agrupador 603 por entrada 613. El generador de bloque transformador 1002 implementa función F tal que genera el bloque transformador WTI a partir del bloque inicial de control R y el bloque de texto aleatorizado-encriptado YI resultado
25 de la aleatorización-encriptación del anterior bloque de texto claro XI. El bloque transformador WTI va adquiriendo los siguientes valores mostrados en la TABLA 1 para los diferentes y sucesivos bloques de texto claro XI ensamblados de una secuencia de texto claro X ; siendo el bloque de texto aleatorizado-encriptado YI_1 el resultado de la aleatorización-encriptación del primer bloque de texto claro XI_1 , el bloque de texto aleatorizado-encriptado YI_2 el resultado de
30 la aleatorización-encriptación del segundo bloque de texto claro XI_2 , y así sucesivamente. Esta secuenciación de bloques de longitud N respecto a la secuencia de texto en particular es también usada en la descripción de los elementos de las Fig.7, Fig.10 y Fig.11.

TABLA 1 - VALORES QUE ADQUIERE WTI

Orden de bloque de texto claro	Bloque de texto claro	Valor de WTI
Primero	XI_1	$F(R)$
Segundo	XI_2	$F(YI_1)$
Tercero	XI_3	$F(YI_2)$
....
N	XI_n	$F(YI_{n-1})$

La función F implementada en el generador de bloque transformador 1002 podría ser definida entre múltiples maneras como:

- $WTI_1 = F(R) = H_1(R)$, para el primer bloque transformador WTI,
- $WTI_n = F(YI_{n-1}) = H_n(R, YI_{n-1})$, para el "enésimo" bloque transformador WTI que se genera para la aleatorización-encryptación del "enésimo" bloque de texto claro XI .

Donde:

- $WTI_1 = H_1(R)$ podría ser:

$WTI = R$, la identidad, o

WTI resultado de cálculos realizados con R , por ejemplo.

y

- $WTI_n = H_n(R, YI_{n-1})$ entre muchas posibles implementaciones:

- Podría ser $H_n(R, YI_{n-1}) = YI_{n-1}$, el anterior bloque de texto aleatorizado-encryptado YI , que aunque se genere una secuencia de texto aleatorizado-encryptado Y aleatoria, presenta respecto a otras implementaciones el inconveniente de que el bloque transformador WTI es conocido, facilitando los ataques criptoanalíticos que se pueden realizar.

- Podría ser $H_n(R, YI_{n-1}) = E_n(R) \text{ oper_1 } YI_{n-1}$:

Donde oper_1 puede ser la operación XOR u Or-exclusiva.

Y $E_n(R)$ podría elegirse para que implementase una de las funciones que se exponen a continuación, por exponer algunas de las posibles y sin que se tenga que limitar a las mismas, como son:

- $E_n(R) = (E_{n-1}(R) + 1) \bmod 2^{64}$, o $E_n(R) = (E_{n-1}(R) - 1) \bmod 2^{64}$.

- Dividido el bloque inicial de control R en dos subbloques $R1$ y $R2$ de longitud de 32 bits cada uno puede implementarse como $E_n(Ri) = (E_{n-1}(Ri) + 1) \bmod 2^{32}$, o $E_n(Ri) = (E_{n-1}(Ri) - 1) \bmod 2^{32}$, para $i=1,2$.

- En general, dividido el bloque inicial de control R en Q subbloques, siendo Q divisor de 64, R_1, \dots, R_Q de longitud de $64/Q$ bits cada uno, puede implementarse como $E_n(R_i) = (E_{n-1}(R_i) \text{ oper_2 } B) \bmod 2^{64/Q}$ para $i=1, \dots, Q$, donde B es un valor, y oper_2 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.

- U otra implementación general, dividido el bloque inicial de control R en diferentes subbloques R_1, \dots, R_D , tales que R_i formado por longitud de Q_i bits, siendo Q_i menor o igual a 64, $E_n(R_i) = (E_{n-1}(R_i) \text{ oper_3 } B) \bmod 2^{Q_i}$ para $i=1, \dots, D$, donde B es un valor, y oper_3 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.

Siendo definida la función “mod” previa como la operación “módulo” tal como se conoce en el arte, tal que “ $a = b \bmod c$ ” donde “a” es el resto de la división entera de “b” por “c”.

En estas implementaciones específicas previamente mostradas preferentemente el bloque inicial de control R es de longitud $G=64$ bits y el bloque de control Kp de 192 bits.

- $E_n(R)$ ser adaptación de generador de números aleatorios, como el aparecido originalmente en “Toward a Universal Random Number Generator”, autor George Marsaglia y Arif Zaman, Florida State University de U.S.A., Report: FSU-SCRI-87-50 (1987), el cual a partir del bloque inicial de control R que le es suministrado como lo que los entendidos en el arte entienden por “seed”, puede ser utilizada para generar bloques de 64 bits de datos aleatorios a ser utilizados como función E_n . Haciendo uso el generador de una “seed” de 32 bits en este caso particular de generador de números aleatorios, preferentemente el bloque inicial de control R es de longitud $G=32$ bits y el bloque de control Kp de 160 bits.

- $E_n(R)$ hacer uso de función de hash MD5, descrita en “Request for Comments: 1321” o “rfc1321”, autor R.Rivest, del MIT Laboratory for Computer Science and RSA Data Security, Inc., U.S.A., del Abril de 1992, la cual a partir del bloque inicial de control R que le es suministrado como datos iniciales, puede ser utilizada para generar bloques de 64 bits a ser utilizados como función E_n , de modo que $E_n(R) = 64$ bits seleccionados de $MD5_n(R)$ y $MD5_n(R) = MD5(MD5_{n-1}(R))$ por ejemplo. Por las características de las funciones de hash, el bloque inicial de control R puede ser de cualquier longitud G, y el bloque de control Kp es preferentemente de $128 + G$ bits.

- $E_n(R)$ hacer uso de función de hash SHA1, objeto de la publicación "Federal Information Processing Standards Publication 180-1" o "FIPS PUB 180-1" del 17 de Abril de 1995, que anuncia el "Secure Hash Standard" del "National Institute of Standards and Technology" ("NIST") del Departamento de Comercio del Gobierno de los Estados Unidos, la cual a partir del bloque inicial de control R que le es suministrado como datos iniciales, puede ser utilizada para generar bloques de 64 bits a ser utilizados como función E_n , de modo que $E_n(R) = 64$ bits seleccionados de $SHA1_n(R)$ y $SHA1_n(R) = SHA1(SHA1_{n-1}(R))$ por ejemplo. El bloque inicial de control R puede ser de cualquier longitud G y el bloque de control Kp es preferentemente de $128 + G$ bits.

- Otras posibles implementaciones de $E_n(R)$.

- Podría ser $H_n(R, YI_{n-1}) = R \text{ oper_4 } E'_n(YI_{n-1})$:

Donde oper_4 puede ser también la operación XOR u Or-exclusiva.

$E'_n(YI_{n-1})$ podría ser, entre las siguientes y sin tener que limitarse a las mismas:

- $E'_n(YI_{n-1}) = (YI_{n-1} + 1) \bmod 2^{64}$, o $E'_n(YI_{n-1}) = (YI_{n-1} - 1) \bmod 2^{64}$.

- Dividido el bloque YI_{n-1} en dos subbloques $YI_{n-1,1}$ y $YI_{n-1,2}$ de longitud de 32 bits cada uno puede implementarse como $E'_n(YI_{n-1,i}) = (YI_{n-1,i} + 1) \bmod 2^{32}$, o $E'_n(YI_{n-1,i}) = (YI_{n-1,i} - 1) \bmod 2^{32}$, para $i=1,2$.

- En general, dividido el bloque YI_{n-1} en Q subbloques, siendo Q divisor de 64, $YI_{n-1,1}, \dots, YI_{n-1,Q}$ de longitud de $64/Q$ bits cada uno, puede implementarse como $E'_n(YI_{n-1,i}) = (YI_{n-1,i} \text{ oper_5 } B) \bmod 2^{64/Q}$, para $i=1, \dots, Q$, donde B es un valor, y oper_5 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.

- O igualmente, otra implementación general, dividido el bloque YI_{n-1} en diferentes subbloques $YI_{n-1,1}, \dots, YI_{n-1,D}$, tales que $YI_{n-1,i}$ formado por longitud de Q_i bits, siendo Q_i menor o igual a 64, $E'_n(YI_{n-1,i}) = (YI_{n-1,i} \text{ oper_6 } B) \bmod 2^{Q_i}$, para $i=1, \dots, D$, donde B es un valor, y oper_6 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.

- Hacer uso de función de hash como MD5 o SHA1, ya mencionadas previamente, tal que $E'_n(YI_{n-1}) = 64$ bits seleccionados de MD5(YI_{n-1}) o 64 bits seleccionados de SHA1(YI_{n-1}).

En estas implementaciones específicas previamente mostradas preferentemente el bloque inicial de control R es de longitud $G=64$ bits y el bloque de control Kp de

192 bits.

- Otras posibles implementaciones de $E'_n(YI_{n-1})$.

- Podría ser $H_n(R, YI_{n-1}) = YI_{n-1} \text{ oper_7 } H_{n-1}(R, YI_{n-2})$ donde por ejemplo:

- oper_7 puede ser también la operación XOR u Or-exclusiva.

- y $H_1(R, YI_0) = R$.

En esta implementación específica preferentemente el bloque inicial de control R es de longitud $G=64$ bits y el bloque de control Kp de 192 bits.

- Otras posibles implementaciones de $WTI_n = F(YI_{n-1}) = H_n(R, YI_{n-1})$.

Obviamente existen y existirán implementaciones específicas de la función F, implementada en el generador de bloque transformador 1002, al igual que con las posibles funciones que implementa el generador autónomo de bloque transformador 5002, que presentan más alta probabilidad que otras funciones F de que el aleatorizador-encryptador produzca texto aleatorizado-encryptado que cumpla con los tests de aleatoriedad implementados en el analizador de aleatoriedad 503 de la Fig.5 en función de la secuencia texto claro \underline{X} que se desee aleatorizar-encryptar con un bloque de control Kp.

La longitud del bloque de control Kp puede ser preferentemente de longitud suma de la longitud del bloque inicial de control Z, preferentemente de 128 bits, y la longitud del bloque inicial de control R, el cual tendrá preferentemente la longitud del bloque inicial de la implementación particular de generador de bloque transformador 1002. Se tiene más seguridad en la confidencialidad de la información aleatorizada-encryptada, pues cuanto mayor es la longitud del bloque de control Kp más se ve incrementado el coste de los ataques por fuerza bruta que pueden llevarse a cabo. La longitud del bloque de control seleccionado Ks es formada por una secuencia mayor de 128 bits, y aunque es actualmente aceptado que 128 bits son suficientes ante ataques enemigos, cuanto mayor es la longitud en bits de la clave utilizada por el dispositivo de encryptación, más segura es la inviolabilidad del texto encryptado que se desea proteger.

La operación de verificación de aleatoriedad de la secuencia de texto aleatorizado-encryptado candidata \underline{Yp} es computacionalmente factible por las mencionadas características de presentar la secuencia de texto aleatorizado-encryptado candidata \underline{Yp} , resultado de la encryptación con la presente invención, substancialmente características propias de las secuencias aleatorias; por lo que el dispositivo de la presente invención presenta la nueva posibilidad de poder medir objetivamente la confusión y difusión de valores que presenta la secuencia de texto aleatorizado-encryptado candidata \underline{Yp} particular por parte de legos en la materia; así como poder diferenciar entre diferentes, y cualesquiera que sean utilizados bloques

de control K_p posibles, cuales nos dan una mayor confusión y difusión de valores.

Además, con el aleatorizador-encryptador, en todas sus variantes, se tiene un generador de números aleatorios; suministrando diferentes datos de entrada como secuencia de texto claro X , texto Y_p que forma una secuencia aleatoria es dada como salida. Esto significa que el dispositivo de aleatorización-encryptación de acuerdo a la invención puede ser usado también como un generador de números aleatorios.

Por la difusión y confusión del texto aleatorizado-encryptado resultado, unido a la influencia que un cambio de un bit en la secuencia de texto claro X conlleva en todos los bits posteriores de salida, puede el dispositivo aleatorizador-encryptador 501, así como su variante 501v1, también ser utilizado como “funcion de hash” o “one-way encryption” como es conocida por aquellos con conocimientos en el arte de la encryptación.

La Fig.7 muestra posible diagrama de descryptador para la descryptación de secuencia de texto aleatorizado-encryptado generada con aleatorizador-encryptador de la Fig.6. En la Fig.7, partes correspondientes a partes de las Fig.1, Fig.4, Fig.5 y Fig.6 son designadas por mismas referencias.

El bloque de control seleccionado K_s llega al divisor de bloque de control 1001 por el canal seguro 108, siendo dividido en bloque inicial de control Z y bloque inicial de control R . El divisor de bloque de control 1001 divide el bloque de control seleccionado K_s de igual modo que el divisor de bloque de control 1001 de la Fig.6 con que se aleatorizó-encryptó la secuencia de texto aleatorizado-encryptado Y_s que es descryptada. El bloque inicial de control Z se suministra por salida 711 al generador de subbloques de control de descryptación 401, el cual genera los cincuenta y dos subbloques de control de descryptación U_1 a U_{52} que se suministran por entrada 311 al encryptador-descryptador 204. El bloque inicial de control R se suministra al generador de bloque transformador 1002 por salida 2010.

El generador de bloque transformador 1002, presenta entradas 2010 y 713, y salida 714, siendo el propósito del generador de bloque transformador 1002, tanto en la Fig.7 como en la Fig.9 y al igual que el generador autónomo de bloque transformador 5002 de las Fig.11 y Fig.13, suministrar el bloque transformador WTJ de longitud $N=64$ bits que se da como entrada del agrupador 603 por entrada 714.

El generador de bloque transformador 1002 implementa función F generadora de bloque transformador WTJ igual a la función F implementada en el generador de bloque transformador 1002 del dispositivo de la Fig.6 con que se generó la secuencia de texto aleatorizado-encryptado Y_s objeto de la descryptación.

La TABLA 2 muestra los diferentes valores que adquiere el bloque transformador WTJ para los diferentes y sucesivos bloques de texto aleatorizado-encryptado YJ desencryptados.

TABLA2 - VALORES QUE ADQUIERE WTJ

Orden de bloque de texto aleatorizado-encryptado	Bloque de texto aleatorizado-encryptado	Valor de WTJ
Primero	YJ_1	$F(R)$
Segundo	YJ_2	$F(YJ_1)$
Tercero	YJ_3	$F(YJ_2)$
....
N	YJ_n	$F(YJ_{n-1})$

5 La secuencia de texto aleatorizado-encryptado Y_s llega continuamente por el canal de transmisión 103 al ensamblador de entrada de bloque de longitud N 301, el cual ensambla bloques de texto aleatorizado-encryptado YJ de longitud preferentemente N=64 bits de la secuencia de texto aleatorizado-encryptado Y_s . El ensamblador de entrada de bloque de longitud N 301 conecta con el encryptador-desencryptador 204 por salida 312, y con la unidad de retención 702 por entrada 712, que puede ser una derivación de la salida 312. El bloque de texto aleatorizado-encryptado YJ se suministra al encryptador-desencryptador 204 y a la unidad de retención 702 por salida 312. El propósito de la unidad de retención 702 es mantener una copia del actual bloque de texto aleatorizado-encryptado YJ que se suministra como entrada del encryptador-desencryptador 204 para la utilización posterior por parte del generador de bloque transformador 1002.

El bloque de texto aleatorizado-encryptado YJ alcanza el encryptador-desencryptador 204, donde es agrupado junto con los cincuenta y dos subbloques de control de desencryptación U_1 a U_{52} , dando un interbloque desencryptado SJ de longitud N=64 bits por salida 313. El agrupador 603 consta de entradas 313 y 714, y salida 715, de 64 líneas paralelas cada una. En el agrupador 603 se agrupan el correspondiente interbloque desencryptado SJ y el correspondiente bloque transformador WTJ, que llegan por entradas 313 y 714 respectivamente, dando el correspondiente bloque de texto claro XJ de longitud N=64 bits. La operación de agrupación que se realiza en el agrupador 603 es la conocida OR-exclusiva o XOR bit a bit de tal modo que $SJ \oplus WTJ \rightarrow XJ$.

25 Este bloque de texto claro XJ se suministra por salida 715 a la unidad de salida de bloque

de longitud N 302. Una vez se tiene el bloque de texto claro XJ , se suministra por entrada 713 el actual bloque de texto aleatorizado-encryptado YJ que contiene la unidad de retención 702 al generador de bloque transformador 1002 para que en la descriptación del siguiente bloque de texto aleatorizado-encryptado YJ ensamblado, el generador de bloque transformador 1002
5 genere el correspondiente bloque transformador WTJ que ha de ser utilizado. Es posible la eliminación de la unidad de retención 702, al igual que en el descriptador de la Fig.9, si el generador de bloque transformador 1002 se implementa de modo que puede recibir el actual bloque de texto aleatorizado-encryptado YJ y utilizarlo en la generación del correspondiente bloque transformador WTJ que será usado en la descriptación del siguiente bloque de texto
10 aleatorizado-encryptado YJ ; ello conllevaría así mismo por ejemplo la eliminación de la entrada/salida 713 y ser entrada del generador de bloque transformador 1002 la entrada 712. Se deja en la Fig.7 y Fig.9 la unidad de retención 702 y la entrada/salida 713 por considerarlo más clarificador de la operativa.

El bloque de texto claro XJ es convertido en una unidad de salida de bloque de longitud N
15 302, pudiendo ser transmitido a la unidad de destino 105, la sucesión de bloques de texto claro XJ forma la secuencia de texto claro \underline{X} .

La Fig.8 muestra posible diagrama de primera variante de aleatorizador-encryptador de secuencia de texto claro de acuerdo con la invención. En la Fig.8, partes correspondientes a
20 partes de las Fig.1, Fig.3, Fig.5 y Fig.6 son designadas por mismas referencias.

Se caracteriza esta variante de aleatorizador-encryptador 501v1 por ser el bloque de control Kp la variante de bloque de control Kpv formada por el bloque inicial de control Z . El bloque de control Kpv llega por canal 107, alcanzando al generador de subbloques de control de encryptación 202, que genera los subbloques de control de encryptación Z_1 a Z_{52} que se
25 suministran por entrada 311 del encryptador-desencryptador 204. El bloque inicial de control R de longitud preferentemente $L2=G$ bits en esta realización está prefijado para la aleatorización-encryptación de una secuencia de texto claro \underline{X} , no depende del bloque de control Kpv .

Para la generación de los bloque transformador WTI el generador de bloque transformador 1002 implementa función F que hace uso del bloque inicial de control R prefijado y el bloque de
30 texto aleatorizado-encryptado YI resultado de la aleatorización-encryptación del anterior bloque de texto claro XI al igual que el generador de bloque transformador 1002 de la Fig.6. La función F que implementa el generador de bloque transformador 1002 puede ser idéntica a cualquiera de las funciones F expuestas previamente en la descripción de la Fig.6; la diferencia con el aleatorizador-encryptador de la Fig.6 estriba en el bloque inicial de control R prefijado, en el

aleatorizador-encryptador de la Fig.6 es suministrado por el divisor de bloque de control 1001, elemento del que carece esta realización.

Aunque en esta variante de aleatorizador-encryptador 501v1, al igual que la variante de aleatorizador-encryptador 501v3 de la Fig.12, el bloque de control Kpv está formada
5 preferentemente por una secuencia de 128 bits, siendo por lo tanto mas “débil”, ante ataques enemigos como puede ser un ataque por “fuerza bruta”, que el bloque de control Kp usado en el aleatorizador-encryptador 501 de la Fig.6 o su variante 501v2 de la Fig.10, es aceptado que actualmente 128 bits de longitud de clave presentan por el momento suficiente seguridad.

No se realiza la descripción completa de la operativa del dispositivo al considerarse que la
10 similitud con la descripción ofrecida en el modo de realización del aleatorizador-encryptador de la Fig.6 y la propia Fig.8, que mantiene referencias comunes, permiten comprender fácilmente cual es el modo de realización del mismo.

La Fig.9 muestra posible diagrama de variante de descryptador para la descryptación
15 de secuencia de texto aleatorizado-encryptado generada con variante de aleatorizador-encryptador de la Fig.8. En la Fig.9, partes correspondientes a partes comunes de las Fig.1, Fig.4, Fig.5, Fig.7 y Fig.8 son designadas por mismas referencias.

El bloque de control seleccionado Ks en esta variante de descryptador 502v1 es la variante de bloque de control seleccionado Ksv formada por el bloque inicial de control Z. El
20 bloque de control seleccionado Ksv llega por el canal seguro 108 y se suministra al generador de subbloques de control de descryptación 401 que genera los subbloques de control de descryptación U_1 a U_{52} que se suministran por entrada 311 al encryptador-descryptador 204.

El bloque inicial de control R de longitud preferentemente $L2=G$ bits en esta realización está prefijado para la descryptación de la secuencia de texto aleatorizado-encryptado \underline{Y}_s , no
25 depende de la variante de bloque de control seleccionado Ksv que se suministra al dispositivo por el canal 108. El generador de bloque transformador 1002 implementa función F, tal que genera los bloques transformador WTJ a partir del bloque inicial de control R prefijado y el bloque de texto aleatorizado-encryptado YJ previamente descryptado. El bloque inicial de control R y la función F específica que implementa el generador de bloque transformador 1002
30 son respectivamente iguales al bloque inicial de control R y a la función F implementada en el generador de bloque transformador 1002 del aleatorizador-encryptador de la Fig.8 con que se aleatorizó-encryptó la secuencia de texto aleatorizado-encryptado \underline{Y}_s objeto de la descryptación actual.

No se realiza la descripción completa del descryptador 502v1 al considerarse que la

similitud con la descripción ofrecida en el modo de realización del descryptador de la Fig.7 y la propia Fig.9, junto con las referencias comunes, permiten comprender cual es el modo de realización del mismo.

5 La Fig.10 muestra posible diagrama de tercera variante de aleatorizador-encryptador de la Fig.5. En la Fig.10, partes correspondientes a partes de las Fig.1, Fig.3, Fig.5 y Fig.6 son designadas por mismas referencias.

Con respecto a la Fig.6 esta variante de aleatorizador-encryptador 501v2, la realización se concreta en la substitución del generador de bloque transformador 1002 por generador
10 autónomo de bloque transformador 5002, y eliminación adicional de conexión 614.

El divisor de bloque de control 1001 presenta entrada 107 y salidas 611 y 1010. El divisor de bloque de control 1001 recibe el bloque de control Kp por canal 107 dividiéndolo en bloque inicial de control Z, de longitud preferentemente $L1=128$ bits, y bloque inicial de control R, de longitud preferentemente $L2=G$ bits. El bloque inicial de control Z se suministra al generador de
15 subbloques de control de encriptación 202 por salida 611. El subbloque inicial de control R se suministra al generador autónomo de bloque transformador 5002 por salida 1010.

El generador autónomo de bloque transformador 5002 implementa función F' , tal que el bloque transformador WTI va adquiriendo los siguientes valores mostrados en la TABLA 3 para los diferentes y sucesivos bloques de texto claro XI ensamblados de una secuencia de texto claro
20 \underline{X} que es aleatorizada-encryptada.

TABLA 3 - VALORES QUE ADQUIERE WTI

Orden de bloque de texto claro	Bloque de texto claro	Valor de WTI
Primero	XI_1	$F'_1(R)$
Segundo	XI_2	$F'_2(R)$
Tercero	XI_3	$F'_3(R)$
....
N	XI_n	$F'_n(R)$

La función F' implementada en el generador autónomo de bloque transformador 5002 puede ser definida entre múltiples maneras como:

- 25
- $WTI_1 = F'_1(R)$, para el primer bloque transformador WTI,
 - $WTI_n = F'_n(R)$, para el "enésimo" bloque transformador WTI que se genera para

la aleatorización-encryptación del “enésimo” bloque de texto claro XI.

Donde:

- $WTI_1 = F'_1(R)$ puede ser:

$WTI = R$, la identidad, o

5 WTI resultado de cálculos realizados con R , por ejemplo.

y

- $WTI_n = F'_n(R)$ puede ser, alguna entre las siguientes implementaciones, y sin tener que limitarse a las mismas:

- $F'_n(R) = (F'_{n-1}(R) + 1) \bmod 2^{64}$, o $F'_n(R) = (F'_{n-1}(R) - 1) \bmod 2^{64}$.

10 - Dividido el bloque R en dos subbloques $R1$ y $R2$ de longitud de 32 bits cada uno puede implementarse como $F'_n(Ri) = (F'_{n-1}(Ri) + 1) \bmod 2^{32}$, o $F'_n(Ri) = (F'_{n-1}(Ri) - 1) \bmod 2^{32}$, para $i=1,2$.

- En general, dividido el bloque R en Q subbloques, siendo Q divisor de 64, $R1, \dots, RQ$ de longitud de $64/Q$ bits cada uno, puede implementarse como $F'_n(Ri) =$
15 $(F'_{n-1}(Ri) \text{ oper_8 } B) \bmod 2^{64/Q}$, para $i=1, \dots, Q$, donde B es un valor, y oper_8 puede ser la adición o la sustracción por ejemplo y sin limitar otras posibles operaciones.

- Otra posible implementación general, dividido el bloque R en diferentes subbloques $R1, \dots, RD$, tales que Ri formado por longitud de Qi bits, siendo Qi menor o igual a 64, $F'_n(Ri) = (F'_{n-1}(Ri) \text{ oper_9 } B) \bmod 2^{Qi}$, para $i=1, \dots, D$, donde B es un valor, y oper_9
20 puede ser la adición o la sustracción por ejemplo, sin limitar otras posibles operaciones.
En estas implementaciones específicas previamente mostradas preferentemente el bloque inicial de control R es de longitud $G=64$ bits y el bloque de control Kp de 192 bits.

- $F'_n(R)$ hacer uso de adaptación de generador de números aleatorios, como el
25 anteriormente mencionado, aparecido originalmente en “Toward a Universal Random Number Generator”, autor George Marsaglia y Arif Zaman, el cual a partir del bloque de control R que le es suministrado como lo que los entendidos en el arte entienden por “seed”, puede ser utilizado para generar bloques de 64 bits aleatorios a ser utilizados como función F' . En este caso preferentemente el bloque inicial de control R es de
30 longitud $G=32$ bits y el bloque de control Kp de 160 bits.

- $F'_n(R)$ hacer uso de función de hash MD5 o SHA1, por ejemplo, la cual a partir del bloque de control R que le es suministrado como datos iniciales, puede ser utilizada para generar bloques de 64 bits, de modo que $F'_n(R) = 64$ bits seleccionados de $MD5_n(R)$ y $MD5_n(R) = MD5(MD5_{n-1}(R))$, o $F'_n(R) = 64$ bits seleccionados de

$SHA1_n(R)$ y $SHA1_n(R) = SHA1(SHA1_{n-1}(R))$, por ejemplo. Por las características de las funciones de hash, preferentemente el bloque inicial de control R puede ser de cualquier longitud G, y el bloque de control Kp es de $128 + G$ bits en este caso.

- Otras posibles implementaciones.

- 5 El generador autónomo de bloque transformador 5002 genera los correspondientes bloques transformador WTI a partir del bloque inicial de control R, sin hacer uso de la realimentación con los bloques de texto aleatorizado-encryptado YI que se dan por salida 313 del encriptador-desencriptador 204.

10 El bloque de control Kp preferentemente puede ser de longitud suma de la longitud del bloque inicial de control Z, preferentemente de 128 bits, y la longitud del bloque inicial de control R, el cual dependerá de la implementación específica del generador autónomo de bloque transformador 5002. Se tiene más seguridad en la confidencialidad de la información aleatorizada-encryptada, cuanto mayor sea la longitud del bloque de control Kp mayor es la seguridad al incrementar el coste de los ataques por fuerza bruta que se pueden realizar.

- 15 No se realiza la descripción completa de la operativa del aleatorizador-encryptador al considerarse que la similitud con la descripción ofrecida en el modo de realización del aleatorizador-encryptador de la Fig.6 y la propia Fig.10, junto con las referencias comunes, permiten comprender cual es el modo de realización del mismo.

- 20 La Fig.11 muestra posible diagrama de variante de desencriptador para la desencriptación de secuencia de texto aleatorizado-encryptado generada con aleatorizador-encryptador de la Fig.10. En la Fig.11, partes correspondientes a partes de las Fig.1, Fig.4, Fig.5, Fig.7 y Fig.10 son designadas por mismas referencias.

- 25 En esta variante de desencriptador 502v2, respecto al desencriptador 502 de la Fig.7, el generador de bloque transformador 1002 se substituye por generador autónomo de bloque transformador 5002, y se eliminan unidad de retención 702 y conexiones 712 y 713.

- 30 El divisor de bloque de control 1001 presenta entrada 108 y salidas 711 y 2010. El divisor de bloque de control 1001 recibe el bloque de control seleccionado Ks por canal seguro 108, dividiéndolo en bloque inicial de control Z y bloque inicial de control R. El divisor de bloque de control 1001 divide el bloque de control seleccionado Ks del mismo modo al que el divisor de bloque de control 1001 del dispositivo de la Fig.10 dividió el bloque de control seleccionado Ks para la aleatorización-encryptación de la secuencia de texto aleatorizado-encryptado Y_s que es desencriptada. El bloque inicial de control Z se suministra al generador de subbloques de control de desencriptación 401 por salida 711, y el bloque inicial de control R se suministra al generador

autónomo de bloque transformador 5002 por salida 2010.

El generador autónomo de bloque transformador 5002 implementa función F' que es la misma función a la función F' que implementa el generador autónomo de bloque transformador 5002 del dispositivo de la Fig.10 con que se aleatorizó-encriptó la secuencia texto aleatorizado-encriptado Y_s objeto de la descryptación.

La TABLA 4 muestra los diferentes valores que adquiere el bloque transformador WTJ para los diferentes y sucesivos bloques de texto aleatorizado-encriptado YJ descryptados.

TABLA 4 - VALORES QUE ADQUIERE WTJ

Orden de bloque de texto aleatorizado-encriptado	Bloque de texto aleatorizado-encriptado	Valor de WTJ
Primero	YJ_1	$F'_1(R)$
Segundo	YJ_2	$F'_2(R)$
Tercero	YJ_3	$F'_3(R)$
....
N	YJ_n	$F'_n(R)$

No se realiza la descripción completa del descryptador 502v2 al considerarse que la similitud con la descripción ofrecida en el modo de realización del descryptador de la Fig.7 y la propia Fig.11, junto con las referencias comunes, permiten comprender cual es el modo de realización del mismo.

La Fig.12 muestra posible diagrama de tercera variante de aleatorizador-encriptador de secuencia de texto claro de acuerdo con la invención. En la Fig.12, partes comunes correspondientes a partes de las Fig.1, Fig.3, Fig.5, Fig.6 y Fig.10 son designadas por mismas referencias.

Se caracteriza esta variante de aleatorizador-encriptador 501v3 por ser el bloque de control Kp la variante de bloque de control Kpv formada por el bloque inicial de control Z. El bloque de control Kpv llega por canal 107, alcanzando al generador de subbloques de control de encriptación 202 que genera los subbloques de control de encriptación Z_1 a Z_{52} que se suministran por entrada 311 al encryptador-descryptador 204. El bloque inicial de control R de longitud preferentemente $L2=G$ bits en esta realización está prefijado para la aleatorización-encryptación de una secuencia de texto claro X , no depende del bloque de control Kpv.

Para la generación de los bloques transformador WTl el generador autónomo de bloque transformador 5002 implementa función F' que hace uso de bloque inicial de control R prefijado. La función F' que implementa el generador autónomo de bloque transformador 5002 puede ser cualquiera de las funciones F' expuestas previamente en la descripción de la Fig.10; la
5 diferencia con el aleatorizador-encryptador de la Fig.10 estriba en que el bloque inicial de control R está prefijado en el aleatorizador-encryptador de la Fig.12, mientras que en el dispositivo de la Fig.10 es suministrado por el divisor de bloque de control 1001, eliminado en esta realización.

No se realiza la descripción completa de la operativa del aleatorizador-encryptador al
10 considerarse que la similitud con las descripciones ofrecidas de los modos de realización del aleatorizador-encryptador de la Fig.6 y Fig.10 con la propia Fig.12, que mantienen referencias comunes, permiten comprender cual es el modo de realización del mismo.

La Fig.13 muestra posible diagrama de variante de descryptador para descryptar
15 secuencia de texto aleatorizado-encryptado generada con variante de aleatorizador-encryptador de la Fig.12. En la Fig.13, partes correspondientes a partes comunes de las Fig.1, Fig.4, Fig.5, Fig.7 y Fig.11 son designadas por mismas referencias.

El bloque de control seleccionado K_s en esta variante de descryptador 502v3 es la variante de bloque de control seleccionado K_{sv} formada por el bloque inicial de control Z. El
20 bloque de control seleccionado K_{sv} llega por el canal seguro 108, y se suministra al generador de subbloques de control de descryptación 401 que genera los subbloques de control de descryptación U_1 a U_{52} que se suministran por entrada 311 al encryptador-descryptador 204. El bloque inicial de control R de longitud preferentemente $L_2=G$ bits en esta realización está prefijado para la descryptación de la secuencia de texto aleatorizado-encryptado Y_s , no
25 depende de la variante de bloque de control seleccionado K_{sv} .

El generador autónomo de bloque transformador 5002 implementa función F' tal que genera los bloques transformador WTJ a partir del bloque inicial de control R, al igual que el generador autónomo de bloque transformador 5002 de la Fig.12. El bloque inicial de control R y la función F' específica que implementa el generador autónomo de bloque transformador 5002
30 son respectivamente iguales al bloque inicial de control R utilizado y a la función F' específica implementada en el generador autónomo de bloque transformador 5002 del dispositivo de la Fig.12 con que se aleatorizó-encryptó la secuencia de texto aleatorizado-encryptado Y_s objeto de la descryptación.

No se realiza la descripción completa del descryptador 502v3 al considerarse que la

similitud con las descripciones ofrecidas en los modos de realización del descryptador de las Fig.7 y Fig.12 y la propia Fig.13, junto con las referencias comunes, permiten comprender cual es el modo de realización del mismo.

5 APLICABILIDAD INDUSTRIAL

La presente invención es especialmente aplicable en comunicaciones secretas, mantenimiento de la confidencialidad de la información, transacciones de comercio electrónico, comunicaciones por correo electrónico y semejantes.

10 La implementación específica de la invención puede ser realizada de muy diferentes modos y puede depender de varios factores como la aplicación que se hará de los mismos, el entorno, la tecnología usada y accesible, etcétera. Una implementación software que se ejecute en computadores electrónicos puede ser dada. Por otra parte, una implementación hardware puede ser también dada en la que las funciones lógicas elementales están en forma de unidades
15 de circuitos independientes que pueden ser contruidos de elementos chip discretos o preferentemente de varios módulos de integración en gran escala ("very large scale integration o VLSI"); microprocesadores usando Memoria Solo de Lectura ("Read Only Memory" o "ROM"), o Memoria Solo de Lectura Programable ("Programmable Read Only Memory" o "PROM"), o Memoria Solo de Lectura Electrónicamente Borrable ("Electronically Erasable
20 Read Only Memory" o "EEROM"); entre muchas implementaciones posibles. La implementación hardware tiene la ventaja sobre la implementación software que puede trabajar substancialmente mas rápido.

Todo cuanto no afecte, altere, cambie o modifique la esencia de la invención descrita será
25 variable a los efectos de esta solicitud de patente; así como se busca reivindicar los más amplios aspectos de la invención de la manera más amplia posible que el solicitante conoce en este momento.

REIVINDICACIONES

1. Sistema de aleatorización-encryptación de secuencia de datos que haciendo uso de bloque de control libremente seleccionable con secuencia de texto claro genera secuencia
5 substancialmente aleatoria caracterizado por incluir:

medios de primera entrada para recibir secuencia de texto claro,

medios de segunda entrada para recibir bloque de control,

medios ensambladores de bloques de longitud N que ensamblan mencionada secuencia de texto claro en multitud de bloques de texto claro,

10 medios divisores de bloque de control que dividen mencionado bloque de control en bloque inicial de control de longitud G y bloque inicial de control de longitud 2N,

medios generadores de bloque transformador que con mencionado bloque inicial de control de longitud G y multitud correspondientes bloques de texto aleatorizado-encryptado generan multitud de bloques transformador,

15 medios generadores de subbloques de control de encryptación que con mencionado bloque inicial de control de longitud 2N generan pluralidad de subbloques de control de encryptación,

medios agrupadores que agrupan correspondiente mencionado bloque de texto claro y correspondiente mencionado bloque transformador, generando interbloque agrupado,

20 medios encryptadores-desencryptadores que encryptan mencionado interbloque agrupado con mencionada pluralidad de subbloques de control de encryptación, generando mencionado bloque de texto aleatorizado-encryptado, donde mencionados medios encryptadores-desencryptadores incluyen encryptador-desencryptador objeto de patente US nº5,214,703,

25 medios suministradores de salida que suministran multitud mencionado bloque de texto aleatorizado-encryptado formando secuencia de texto aleatorizado-encryptado,

por lo cual mencionada secuencia de texto aleatorizado-encryptado corresponde a mencionada secuencia de texto claro recibida por mencionados medios de primera entrada,

30 por lo cual mencionada secuencia de texto aleatorizado-encryptado es substancialmente aleatoria,

por lo cual es medurable objetivamente la difusión y confusión de valores de mencionada secuencia de texto aleatorizado-encryptado,

por lo cual es medurable la difusión y confusión de valores introducidas por mencionado bloque de control recibido por mencionados medios de segunda entrada.

2. Sistema de aleatorización-encryptación de secuencia de datos que haciendo uso de bloque de control a partir de secuencia de texto aleatorizado-encryptado recupera secuencia de texto claro caracterizado por incluir:

medios de primera entrada para recibir secuencia de texto aleatorizado-encryptado,

5 medios de segunda entrada para recibir bloque de control,

medios ensambladores de bloques de longitud N que ensamblan mencionada secuencia de texto aleatorizado-encryptado en multitud bloques de texto aleatorizado-encryptado,

medios divisores de bloque de control que dividen mencionado bloque de control en bloque inicial de control de longitud G y bloque inicial de control de longitud $2N$,

10 medios generadores de bloque transformador que con mencionado bloque inicial de control de longitud G y multitud correspondiente anterior mencionado bloque de texto aleatorizado-encryptado ensamblado en mencionados medios ensambladores de bloques de longitud N , generan multitud de bloques transformador,

medios generadores de subbloques de control de desencryptación que con mencionado
15 bloque inicial de control de longitud $2N$ generan pluralidad de subbloques de control de desencryptación,

medios encryptadores-desencryptadores que desencryptan mencionado bloque de texto aleatorizado-encryptado con mencionada pluralidad de subbloques de control de desencryptación, generando interbloque desencryptado, donde mencionados medios
20 encryptadores-desencryptadores incluyen encryptador-desencryptador objeto de patente US nº5,214,703,

medios agrupadores que agrupan mencionado interbloque desencryptado y mencionado bloque transformador, generando bloque de texto claro,

medios suministradores de salida que suministran multitud mencionado bloque de texto
25 claro formando secuencia de texto claro,

por lo cual mencionada secuencia de texto claro corresponde a mencionada secuencia de texto aleatorizado-encryptado recibida por mencionados medios de primera entrada.

3. Sistema de aleatorización-encryptación de secuencia de datos que haciendo uso de bloque
30 inicial de control de longitud $2N$ libremente seleccionable con secuencia de texto claro genera secuencia substancialmente aleatoria caracterizado por incluir:

medios de primera entrada para recibir secuencia de texto claro,

medios de segunda entrada para recibir bloque inicial de control de longitud $2N$,

medios ensambladores de bloques de longitud N que ensamblan mencionada secuencia

de texto claro en multitud de bloques de texto claro,

medios generadores de bloque transformador que con bloque inicial de control de longitud G y multitud correspondientes bloques de texto aleatorizado-encryptado generan multitud de bloques transformador,

5 medios generadores de subbloques de control de encriptación que con mencionado bloque inicial de control de longitud $2N$ generan pluralidad de subbloques de control de encriptación,

medios agrupadores que agrupan correspondiente mencionado bloque de texto claro con correspondiente mencionado bloque transformador, generando interbloque agrupado,

10 medios encriptadores-desencriptadores que encriptan mencionado interbloque agrupado con mencionada pluralidad de subbloques de control de encriptación, generando mencionado bloque de texto aleatorizado-encryptado, donde mencionados medios encriptadores-desencriptadores incluyen encriptador-desencriptador objeto de patente US nº5,214,703,

15 medios suministradores de salida que suministran multitud mencionado bloque de texto aleatorizado-encryptado formando secuencia de texto aleatorizado-encryptado,

por lo cual mencionada secuencia de texto aleatorizado-encryptado corresponde a mencionada secuencia de texto claro recibida por mencionados medios de primera entrada,

20 por lo cual mencionada secuencia de texto aleatorizado-encryptado es substancialmente aleatoria,

por lo cual es medurable objetivamente la difusión y confusión de valores de mencionada secuencia de texto aleatorizado-encryptado,

por lo cual es medurable la difusión y confusión de valores introducidas por mencionado bloque inicial de control de longitud $2N$ recibido por mencionados medios de segunda entrada.

25

4. Sistema de aleatorización-encryptación de secuencia de datos que haciendo uso de bloque inicial de control de longitud $2N$ a partir de secuencia de texto aleatorizado-encryptado recupera secuencia de texto claro caracterizado por incluir:

medios de primera entrada para recibir secuencia de texto aleatorizado-encryptado,

30 medios de segunda entrada para recibir bloque inicial de control de longitud $2N$,

medios ensambladores de bloques de longitud N que ensamblan mencionada secuencia de texto aleatorizado-encryptado en multitud bloques de texto aleatorizado-encryptado,

medios generadores de bloque transformador que con bloque inicial de control de longitud G y multitud correspondiente anterior mencionado bloque de texto aleatorizado-

encriptado ensamblado en mencionados medios ensambladores de bloques de longitud N, generan multitud de bloques transformador,

medios generadores de subbloques de control de descryptación que con mencionado bloque inicial de control de longitud 2N generan pluralidad de subbloques de control de descryptación,

medios encriptadores-descryptadores que descryptan mencionado bloque de texto aleatorizado-encriptado con mencionada pluralidad de subbloques de control de descryptación, generando interbloque descryptado, donde mencionados medios encriptadores-descryptadores incluyen encriptador-descryptador objeto de patente US nº5,214,703,

medios agrupadores que agrupan mencionado interbloque descryptado y mencionado bloque transformador, generando bloque de texto claro,

medios suministradores de salida que suministran multitud mencionado bloque de texto claro formando secuencia de texto claro,

por lo cual mencionada secuencia de texto claro corresponde a mencionada secuencia de texto aleatorizado-encriptado recibida por mencionados medios de primera entrada.

5. Sistema de acuerdo con la reivindicación 1, o 2, o 3, o 4, caracterizado porque mencionados medios generadores de bloque transformador generan mencionado bloque transformador implementando función H (mencionado bloque inicial de control de longitud G, mencionado bloque de texto aleatorizado-encriptado).

6. Sistema de acuerdo con la reivindicación 5 caracterizado porque mencionados medios agrupadores incluyen operación OR-exclusiva.

7. Sistema de acuerdo con la reivindicación 6 caracterizado porque mencionados medios generadores de bloque transformador implementan mencionada función H (mencionado bloque inicial de control de longitud G, mencionado bloque de texto aleatorizado-encriptado) para enésimo mencionado bloque transformador igual a enésimo bloque de longitud N generado por función E_n (mencionado bloque inicial de control de longitud G) XOR enésimo menos uno mencionado bloque de texto aleatorizado-encriptado.

8. Sistema de acuerdo con la reivindicación 7 caracterizado porque mencionados medios generadores de bloque transformador implementan mencionada función E_n (mencionado bloque

inicial de control de longitud G) como $E_n(R_i) = (E_{n-1}(R_i) \text{ oper } B) \bmod 2^{Q_i}$, donde mencionado Q_i menor o igual que 64, mencionado R_i de longitud mencionado Q_i es subbloque de mencionado bloque inicial de control de longitud G, mencionado oper operación aritmética seleccionada del grupo consistente de adición y substracción y desplazamiento, mencionado B valor, mencionado mod operación módulo.

9. Sistema de acuerdo con la reivindicación 8 caracterizado porque mencionado bloque inicial de control de longitud $2N$ formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

10. Sistema de acuerdo con la reivindicación 7 caracterizado porque mencionados medios generadores de bloque transformador implementan mencionada función E_n (mencionado bloque inicial de control de longitud G) incluyendo generador de números aleatorios.

11. Sistema de acuerdo con la reivindicación 10 caracterizado porque mencionado bloque inicial de control de longitud $2N$ formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por longitud de semilla de mencionado generador de números aleatorios.

12. Sistema de acuerdo con la reivindicación 7 caracterizado porque mencionados medios generadores de bloque transformador implementan mencionada función E_n (mencionado bloque inicial de control de longitud G) incluyendo función de hash.

13. Sistema de acuerdo con la reivindicación 12 caracterizado porque mencionado bloque inicial de control de longitud $2N$ formado preferentemente por 128 bits y mencionado bloque de control inicial de longitud G formado preferentemente por cero o más bits.

14. Sistema de acuerdo con la reivindicación 6 caracterizado porque mencionados medios generadores de bloque transformador implementan mencionada función H (mencionado bloque inicial de control de longitud G, mencionado bloque de texto aleatorizado-encryptado) como

para primer mencionado bloque transformador incluye mencionado bloque inicial de control de longitud G,

para enésimo mencionado bloque transformador es igual a enésimo menos uno mencionado bloque de texto aleatorizado-encryptado XOR enésimo menos uno

mencionado bloque transformador.

15. Sistema de acuerdo con la reivindicación 14 caracterizado porque mencionado bloque inicial de control de longitud $2N$ formado preferentemente por 128 bits y mencionado bloque
5 inicial de control de longitud G formado preferentemente por 64 bits.

16. Sistema de acuerdo con la reivindicación 6 caracterizado porque mencionados medios generadores de bloque transformador implementan mencionada función H (mencionado bloque inicial de control de longitud G , mencionado bloque de texto aleatorizado-encryptado) como
10 para primer mencionado bloque transformador es mencionado bloque inicial de control de longitud G ,
para enésimo mencionado bloque transformador es enésimo menos uno mencionado bloque de texto aleatorizado-encryptado.

15 17. Sistema de acuerdo con la reivindicación 16 caracterizado porque mencionado bloque inicial de control de longitud $2N$ formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

18. Sistema de acuerdo con la reivindicación 6 caracterizado porque mencionados medios
20 generadores de bloque transformador implementan mencionada función H (mencionado bloque inicial de control de longitud G , mencionado bloque de texto aleatorizado-encryptado) para enésimo mencionado bloque transformador igual a enésimo bloque de longitud N generado por función E_n (enésimo menos uno mencionado bloque de texto aleatorizado-encryptado) XOR mencionado bloque inicial de control de longitud G .

25 19. Sistema de acuerdo con la reivindicación 18 caracterizado porque mencionados medios generadores de bloque transformador implementan mencionada función E_n (enésimo menos uno mencionado bloque de texto aleatorizado-encryptado) como $E_n (Y_{li}) = (E_{n-1} (Y_{li}) \text{ oper } B) \bmod 2^{Q_i}$, donde mencionado Q_i menor o igual que 64, mencionado Y_{li} de longitud mencionado
30 Q_i es subbloque de mencionado enésimo menos uno mencionado bloque de texto aleatorizado-encryptado, mencionado oper operación aritmética seleccionada del grupo consistente de adición y substracción y desplazamiento, mencionado B valor, mencionado mod operación módulo.

20. Sistema de acuerdo con la reivindicación 19 caracterizado porque mencionado bloque

inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

21. Sistema de acuerdo con la reivindicación 18 caracterizado porque mencionados medios
5 generadores de bloque transformador implementan mencionada función E_n (enésimo menos uno mencionado bloque de texto aleatorizado-encryptado) incluyendo función de hash.

22. Sistema de acuerdo con la reivindicación 21 caracterizado porque mencionado bloque
10 inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque de control inicial de longitud G formado preferentemente por cero o más bits.

23. Sistema de aleatorización-encryptación de secuencia de datos que haciendo uso de bloque de control libremente seleccionable con secuencia de texto claro genera secuencia substancialmente aleatoria caracterizado por incluir:

15 medios de primera entrada para recibir secuencia de texto claro,
 medios de segunda entrada para recibir bloque de control,
 medios ensambladores de bloques de longitud N que ensamblan mencionada secuencia de texto claro en multitud de bloques de texto claro,
 medios divisores de bloque de control que dividen mencionado bloque de control en
20 bloque inicial de control de longitud G y bloque inicial de control de longitud 2N,
 medios generadores autónomos de bloque transformador que con mencionado bloque inicial de control de longitud G generan multitud de bloques transformador,
 medios generadores de subbloques de control de encryptación que con mencionado bloque inicial de control de longitud 2N generan pluralidad de subbloques de control de
25 encryptación,
 medios agrupadores que agrupan correspondiente mencionado bloque de texto claro y correspondiente mencionado bloque transformador, generando interbloque agrupado,
 medios encryptadores-desencryptadores que encryptan mencionado interbloque agrupado con mencionada pluralidad de subbloques de control de encryptación, generando bloque de
30 texto aleatorizado-encryptado, donde mencionados medios encryptadores-desencryptadores incluyen encryptador-desencryptador objeto de patente US nº5,214,703,
 medios suministradores de salida que suministran multitud mencionado bloque de texto aleatorizado-encryptado formando secuencia de texto aleatorizado-encryptado,
por lo cual mencionada secuencia de texto aleatorizado-encryptado corresponde a mencionada

secuencia de texto claro recibida por mencionados medios de primera entrada,
por lo cual mencionada secuencia de texto aleatorizado-encryptado es substancialmente aleatoria,
por lo cual es medurable objetivamente la difusión y confusión de valores de mencionada
5 secuencia de texto aleatorizado-encryptado,
por lo cual es medurable la difusión y confusión de valores introducidas por mencionado bloque de control recibido por mencionados medios de segunda entrada.

24. Sistema de aleatorización-encryptación de secuencia de datos que haciendo uso de bloque
10 de control a partir de secuencia de texto aleatorizado-encryptado recupera secuencia de texto claro caracterizado por incluir:

medios de primera entrada para recibir secuencia de texto aleatorizado-encryptado,
medios de segunda entrada para recibir bloque de control,
medios ensambladores de bloques de longitud N que ensamblan mencionada secuencia
15 de texto aleatorizado-encryptado en multitud bloques de texto aleatorizado-encryptado,
medios divisores de bloque de control que dividen mencionado bloque de control en bloque inicial de control de longitud G y bloque inicial de control de longitud 2N,
medios generadores autónomos de bloque transformador que con mencionado bloque inicial de control de longitud G generan multitud de bloques transformador,
20 medios generadores de subbloques de control de descryptación que con mencionado bloque inicial de control de longitud 2N generan pluralidad de subbloques de control de descryptación,
medios encryptadores-descryptadores que descryptan mencionado bloque de texto aleatorizado-encryptado con mencionada pluralidad de subbloques de control de descryptación, generando interbloque descryptado, donde mencionados medios
25 encryptadores-descryptadores incluyen encryptador-descryptador objeto de patente US n°5,214,703,
medios agrupadores que agrupan mencionado interbloque descryptado y mencionado bloque transformador, generando bloque de texto claro,
30 medios suministradores de salida que suministran multitud mencionado bloque de texto claro formando secuencia de texto claro,

por lo cual mencionada secuencia de texto claro corresponde a mencionada secuencia de texto aleatorizado-encryptado recibida por mencionados medios de primera entrada.

25. Sistema de aleatorización-encryptación de secuencia de datos que haciendo uso de bloque inicial de control de longitud $2N$ libremente seleccionable con secuencia de texto claro genera secuencia substancialmente aleatoria caracterizado por incluir:

medios de primera entrada para recibir secuencia de texto claro,

5 medios de segunda entrada para recibir bloque inicial de control de longitud $2N$,

medios ensambladores de bloques de longitud N que ensamblan mencionada secuencia de texto claro en multitud de bloques de texto claro,

medios generadores autónomos de bloque transformador que con bloque inicial de control de longitud G generan multitud de bloques transformador,

10 medios generadores de subbloques de control de encryptación que con mencionado bloque inicial de control de longitud $2N$ generan pluralidad de subbloques de control de encryptación,

medios agrupadores que agrupan correspondiente mencionado bloque de texto claro y correspondiente mencionado bloque transformador, generando interbloque agrupado,

15 medios encryptadores-desencryptadores que encryptan mencionado interbloque agrupado con mencionada pluralidad de subbloques de control de encryptación, generando bloque de texto aleatorizado-encryptado, donde mencionados medios encryptadores-desencryptadores incluyen encryptador-desencryptador objeto de patente US nº5,214,703,

medios suministradores de salida que suministran multitud mencionado bloque de texto aleatorizado-encryptado formando secuencia de texto aleatorizado-encryptado,

20 por lo cual mencionada secuencia de texto aleatorizado-encryptado corresponde a mencionada secuencia de texto claro recibida por mencionados medios de primera entrada,

por lo cual mencionada secuencia de texto aleatorizado-encryptado es substancialmente aleatoria,

25 por lo cual es medurable objetivamente la difusión y confusión de valores de mencionada secuencia de texto aleatorizado-encryptado,

por lo cual es medurable la difusión y confusión de valores introducidas por mencionado bloque inicial de control de longitud $2N$ recibido por mencionados medios de segunda entrada.

30 26. Sistema de aleatorización-encryptación de secuencia de datos que haciendo uso de bloque inicial de control de longitud $2N$ a partir de secuencia de texto aleatorizado-encryptado recupera secuencia de texto claro caracterizado por incluir:

medios de primera entrada para recibir secuencia de texto aleatorizado-encryptado,

medios de segunda entrada para recibir bloque inicial de control de longitud $2N$,

medios ensambladores de bloques de longitud N que ensamblan mencionada secuencia de texto aleatorizado-encryptado en multitud bloques de texto aleatorizado-encryptado,

medios generadores autónomos de bloque transformador que con bloque inicial de control de longitud G generan multitud de bloques transformador,

5 medios generadores de subbloques de control de descryptación que con mencionado bloque inicial de control de longitud 2N generan pluralidad de subbloques de control de descryptación,

10 medios encryptadores-descryptadores que descryptan mencionado bloque de texto aleatorizado-encryptado con mencionada pluralidad de subbloques de control de descryptación, generando interbloque descryptado, donde mencionados medios encryptadores-descryptadores incluyen encryptador-descryptador objeto de patente US nº5.214,703,

medios agrupadores que agrupan mencionado interbloque descryptado y mencionado bloque transformador , generando bloque de texto claro,

15 medios suministradores de salida que suministran multitud mencionado bloque de texto claro formando secuencia de texto claro,

por lo cual mencionada secuencia de texto claro corresponde a mencionada secuencia de texto aleatorizado-encryptado recibida por mencionados medios de primera entrada.

20 27. Sistema de acuerdo con la reivindicación 23, o 24, o 25, o 26, caracterizado porque mencionados medios generadores de bloque transformador generan mencionado bloque transformador implementando función H (mencionado bloque inicial de control de longitud G).

25 28. Sistema de acuerdo con la reivindicación 27 caracterizado porque mencionados medios agrupadores incluyen operación OR-exclusiva.

29. Sistema de acuerdo con la reivindicación 28 caracterizado porque mencionados medios generadores autónomos de bloque transformador implementan mencionada función H (mencionado bloque inicial de control de longitud G) para enésimo mencionado bloque transformador como $H_n(R_i) = (H_{n-1}(R_i) \text{ oper } B) \bmod 2^{Q_i}$, donde mencionado Q_i menor o igual que 64, mencionado R_i de longitud mencionado Q_i es subbloque de mencionado bloque inicial de control de longitud G, mencionado oper operación aritmética seleccionada del grupo consistente de adición y substracción y desplazamiento, mencionado B valor, mencionado mod operación módulo.

30

30. Sistema de acuerdo con la reivindicación 29 caracterizado porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por 64 bits.

5 31. Sistema de acuerdo con la reivindicación 28 caracterizado porque mencionados medios generadores autónomos de bloque transformador implementan mencionada función H (mencionado bloque inicial de control de longitud G) incluyendo generador de números aleatorios.

10 32. Sistema de acuerdo con la reivindicación 31 caracterizado porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de control de longitud G formado preferentemente por longitud de semilla de mencionado generador de números aleatorios.

15 33. Sistema de acuerdo con la reivindicación 28 caracterizado porque mencionados medios generadores autónomos de bloque transformador implementan mencionada función H (mencionado bloque inicial de control de longitud G) incluyendo función de hash.

20 34. Sistema de acuerdo con la reivindicación 33 caracterizado porque mencionado bloque inicial de control de longitud 2N formado preferentemente por 128 bits y mencionado bloque inicial de longitud G formado por cero o más bits.

1/12

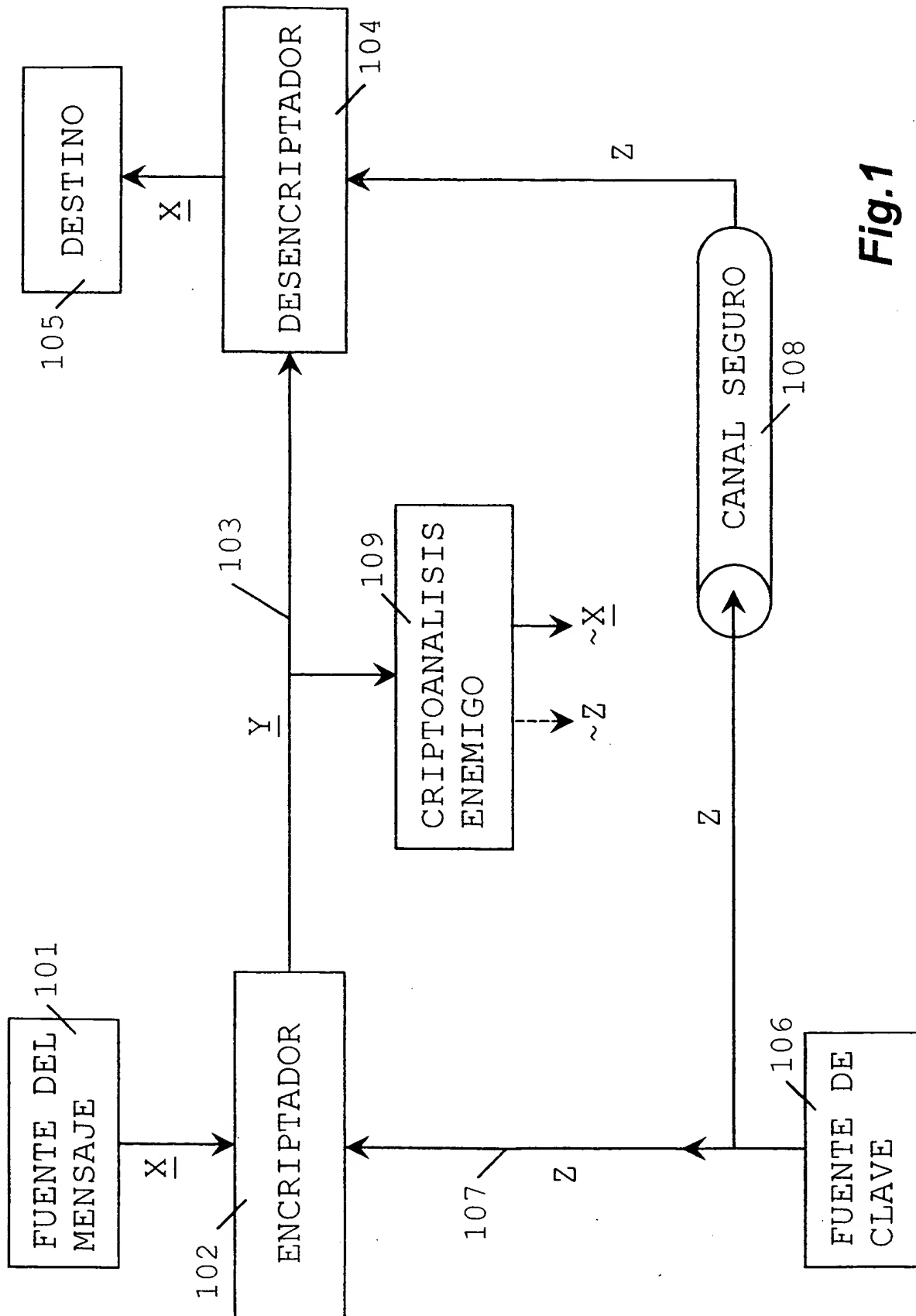
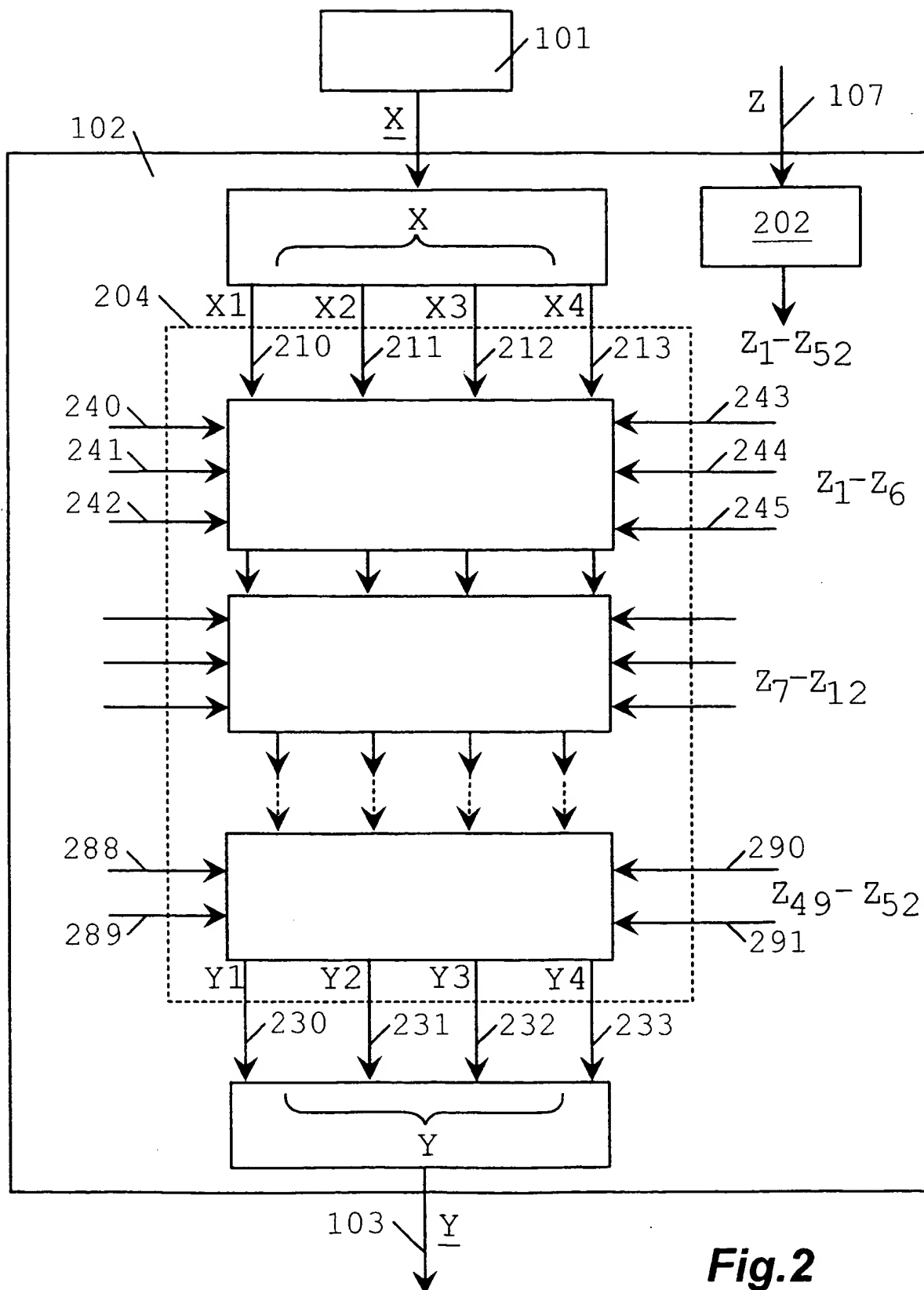


Fig.1

2/12

**Fig.2**

3/12

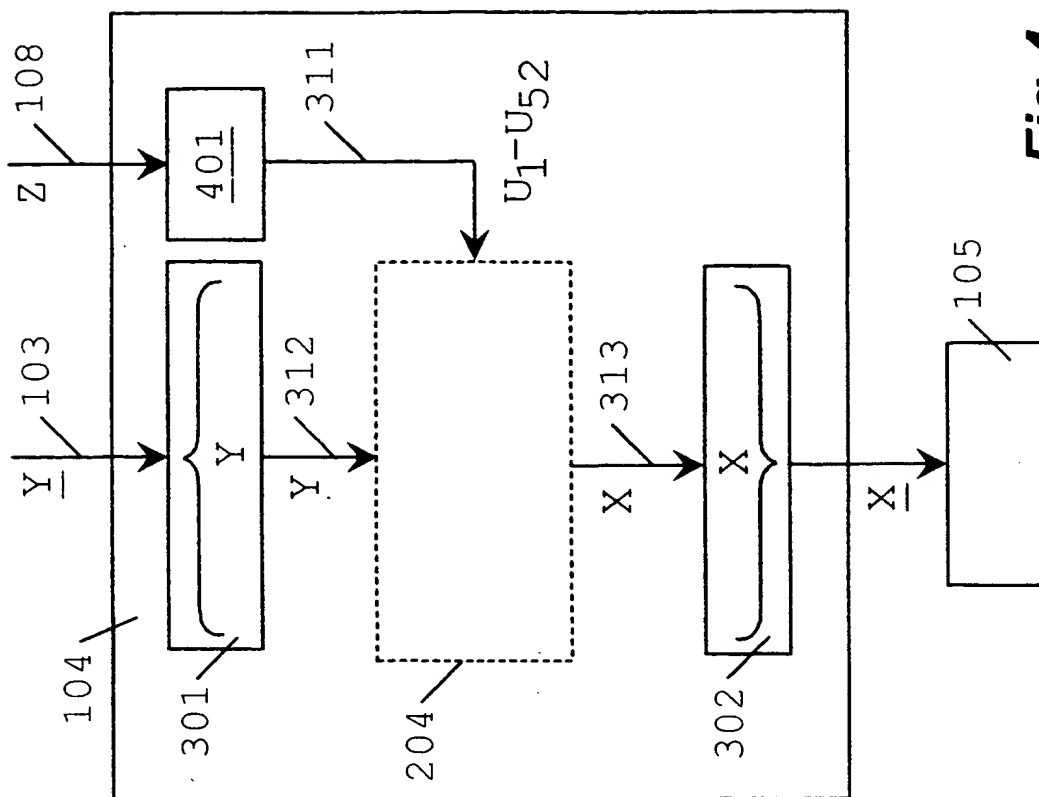


Fig. 4

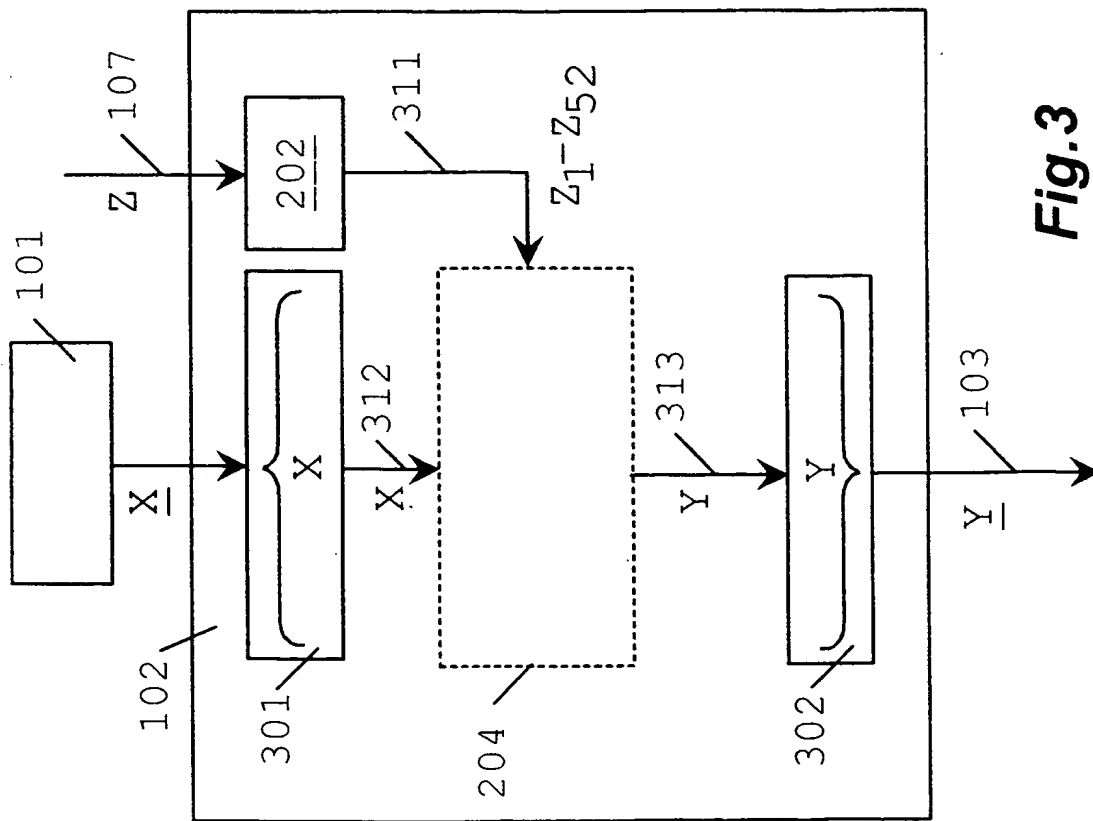
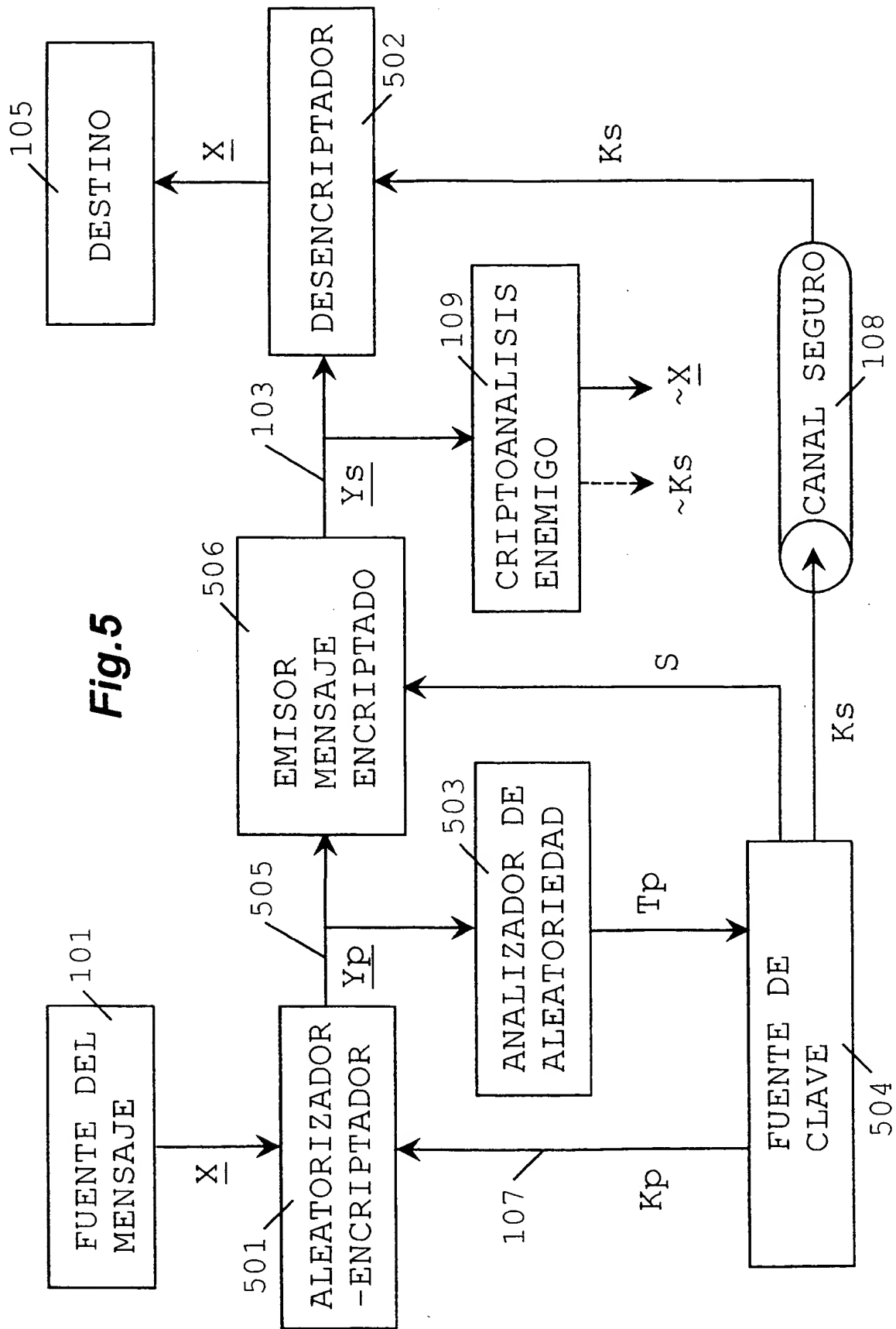
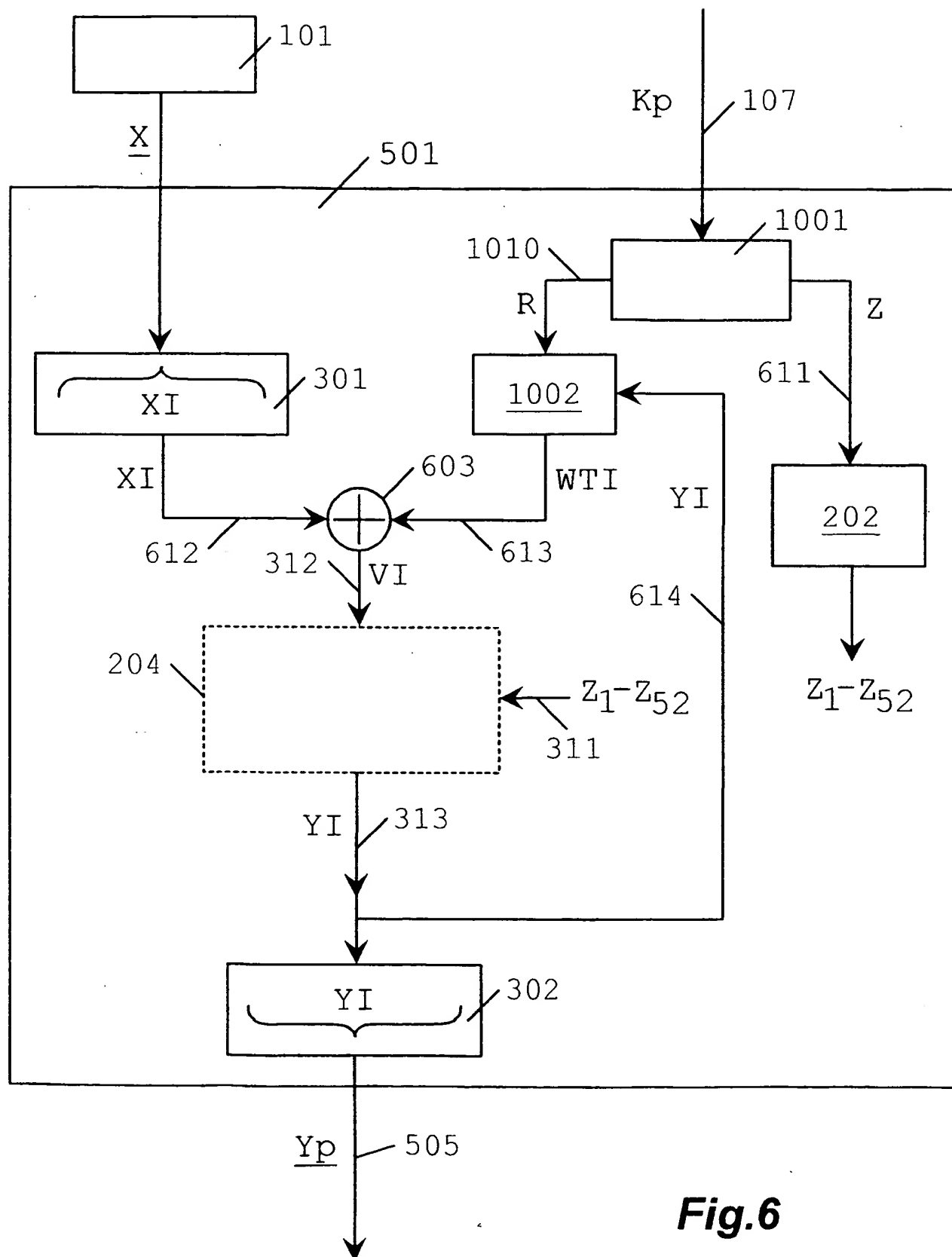


Fig. 3

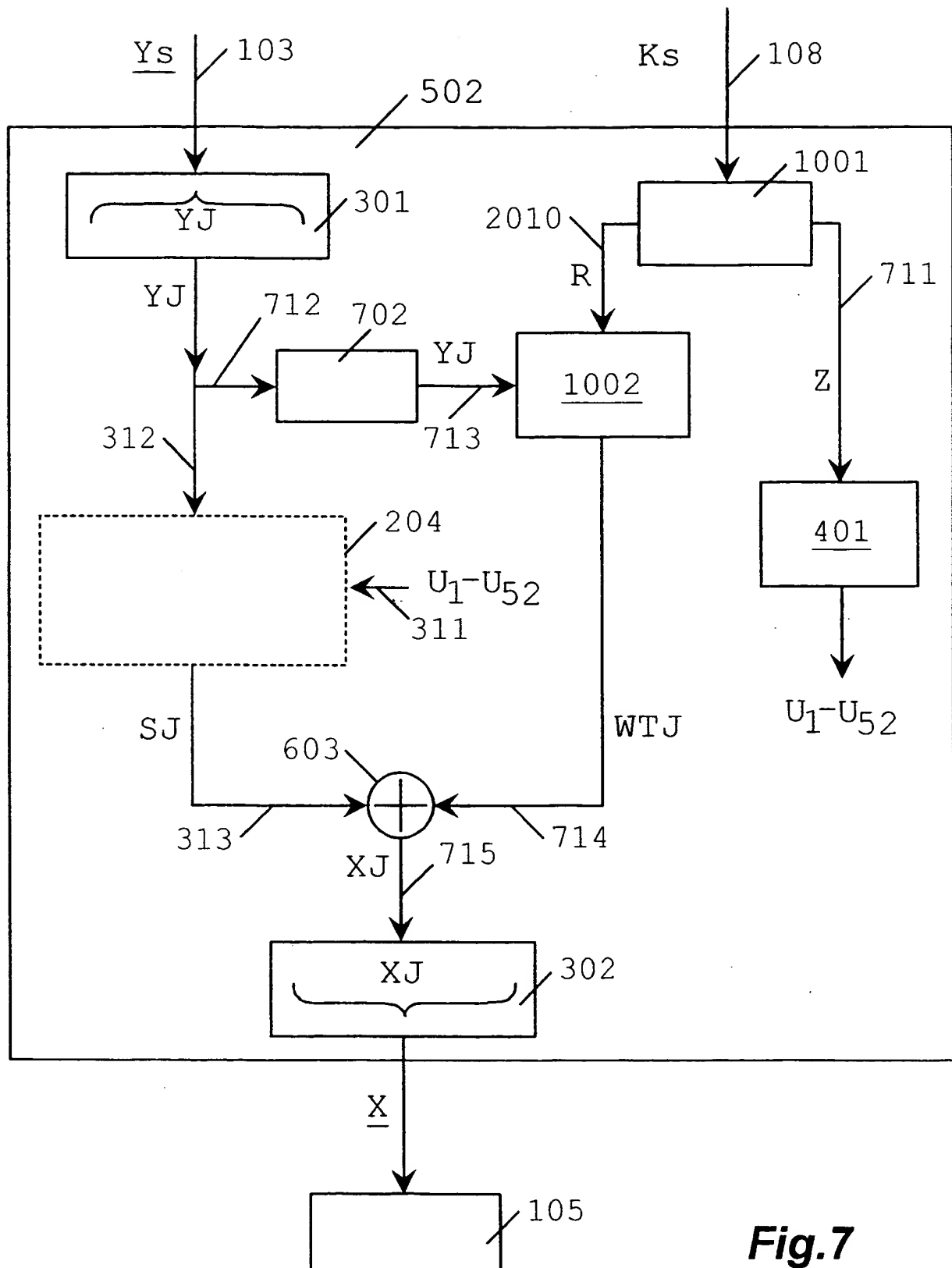
4/12



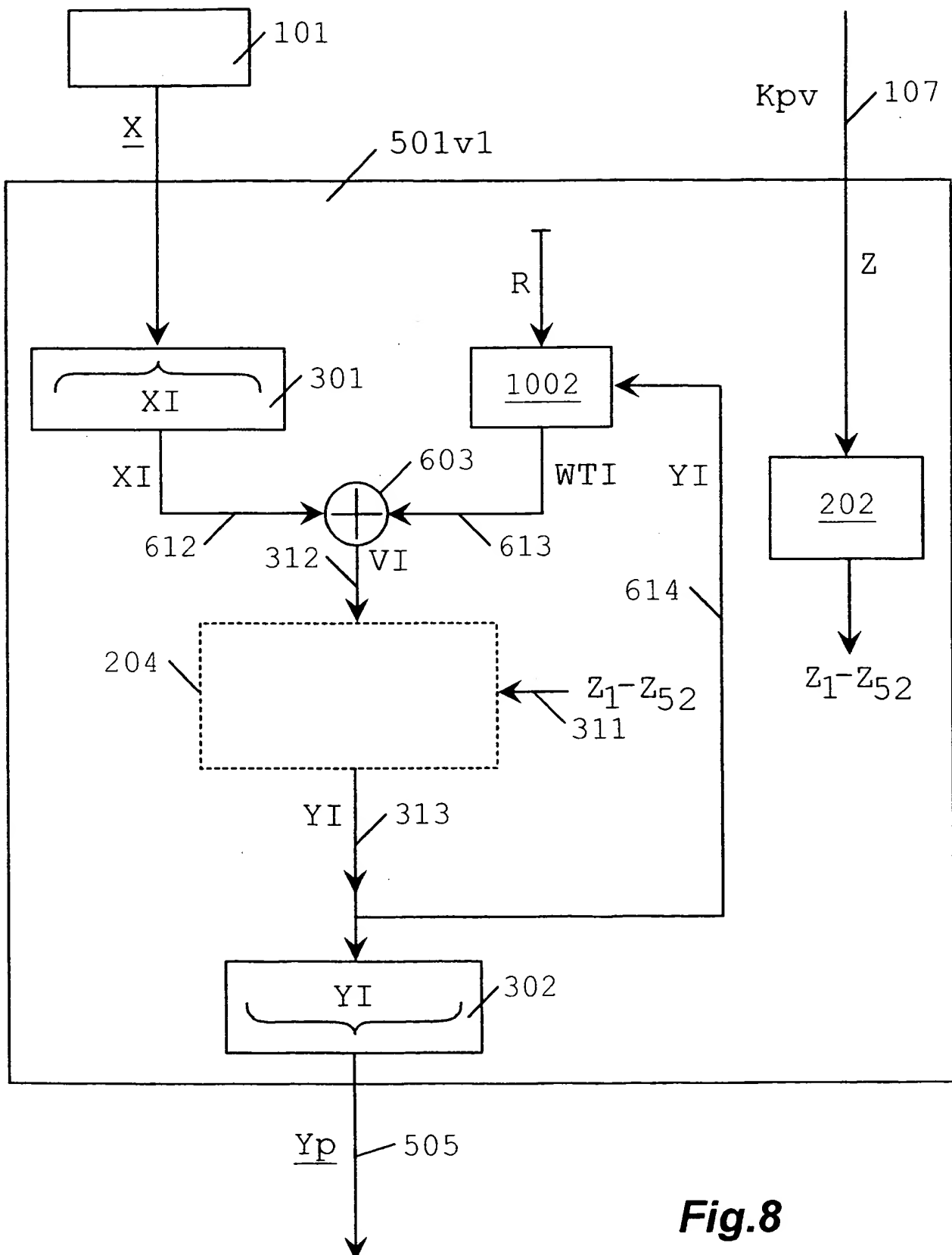
5/12

**Fig.6**

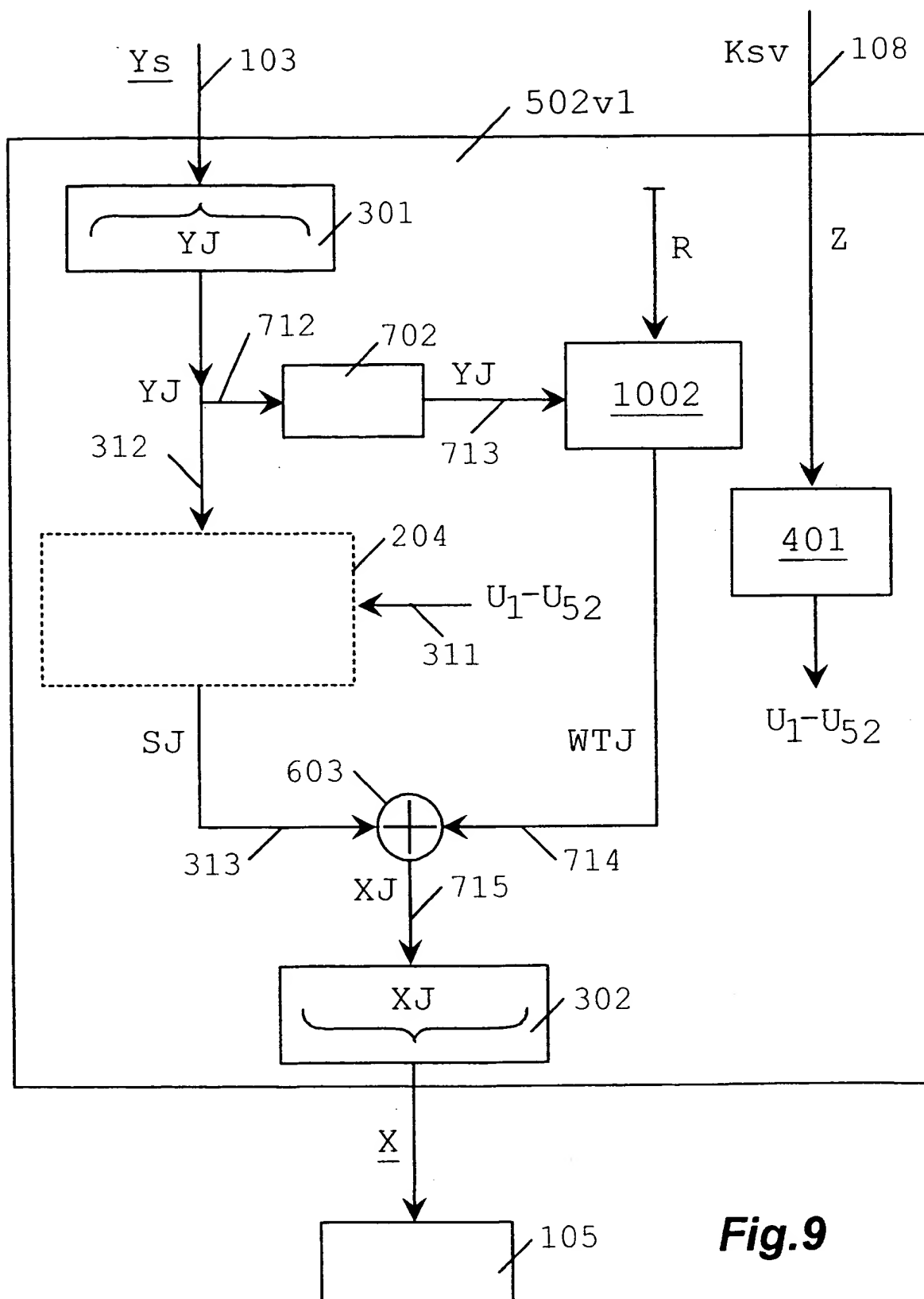
6/12

**Fig.7**

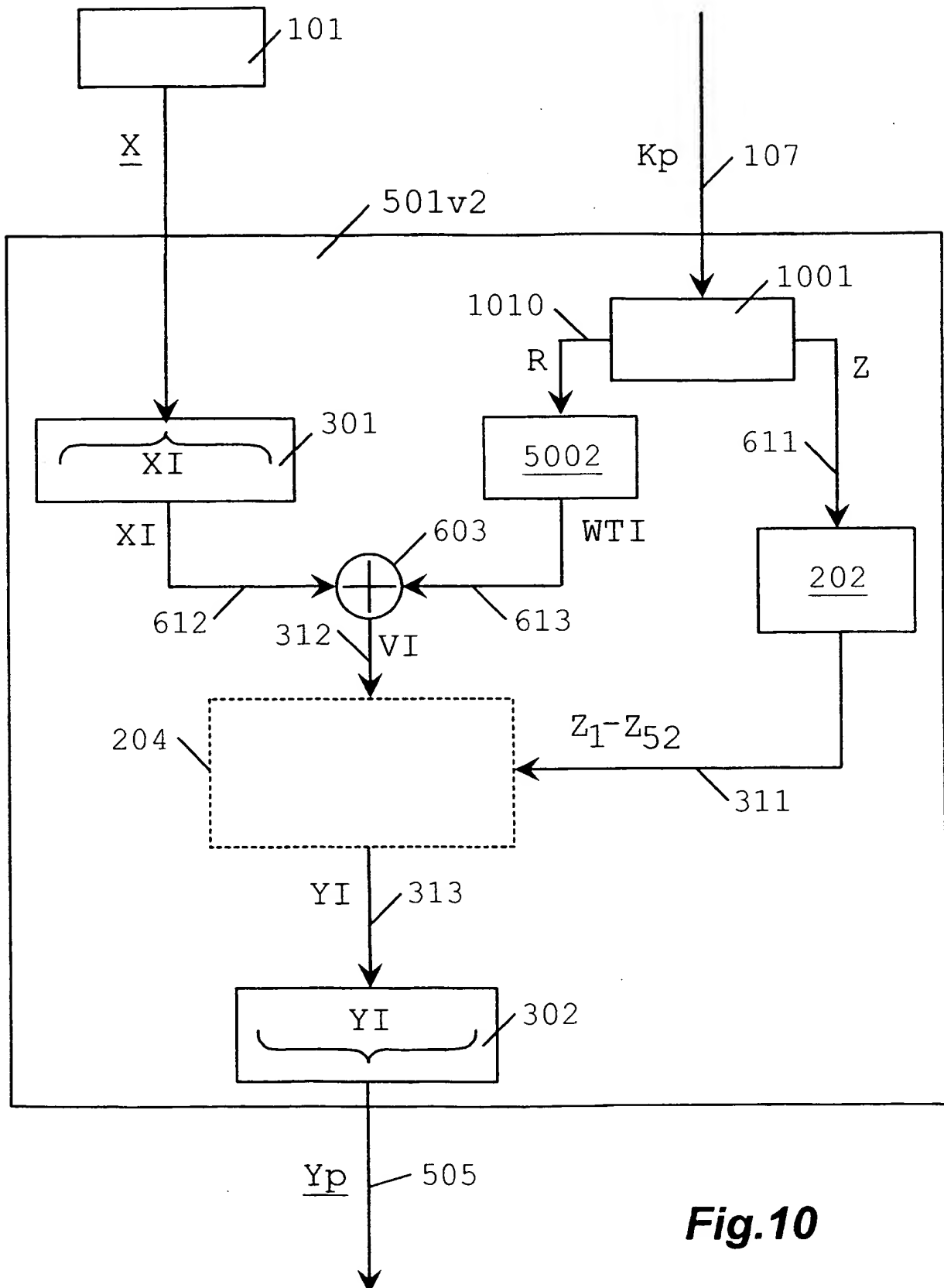
7/12

**Fig.8**

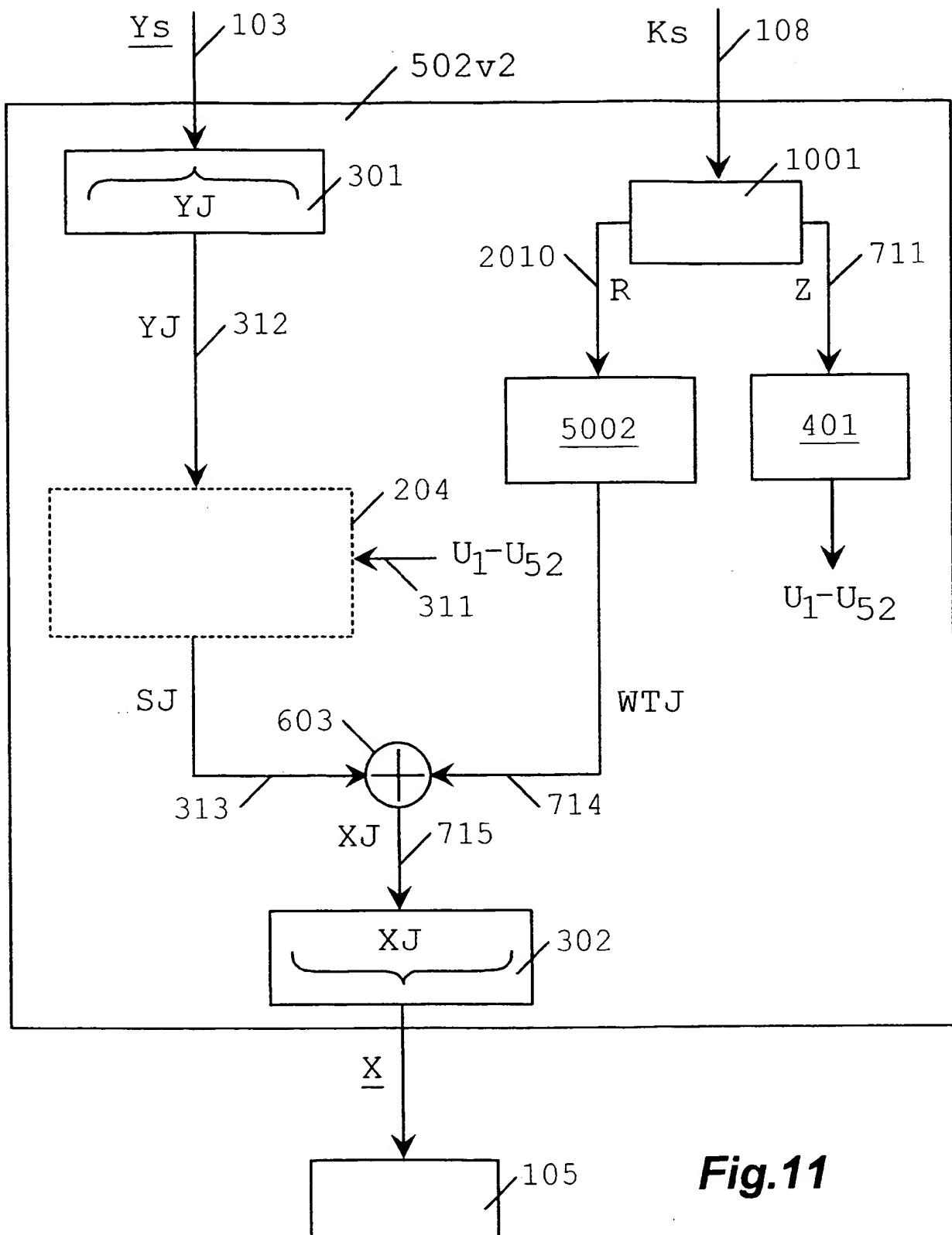
8/12

**Fig.9**

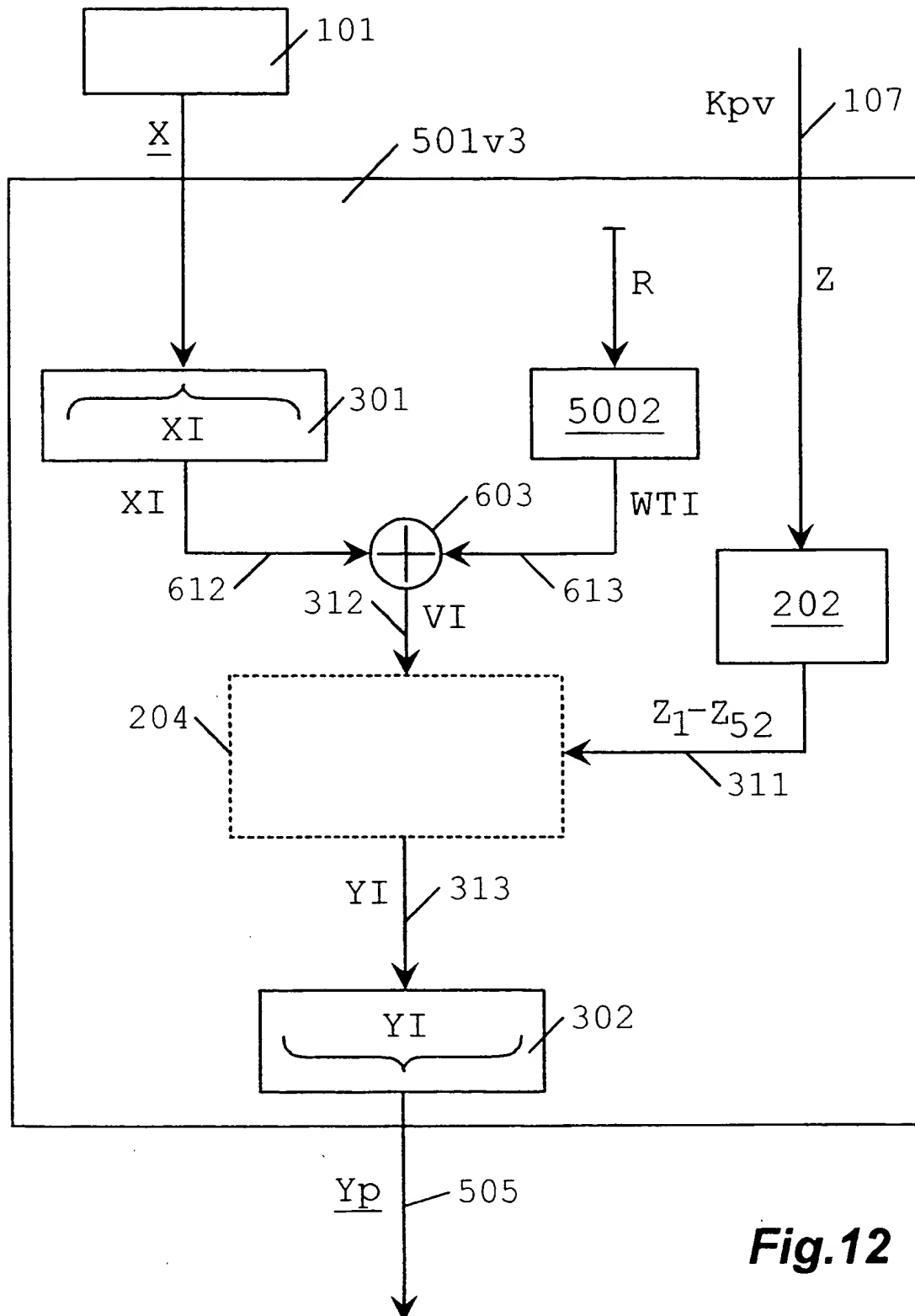
9/12

**Fig.10**

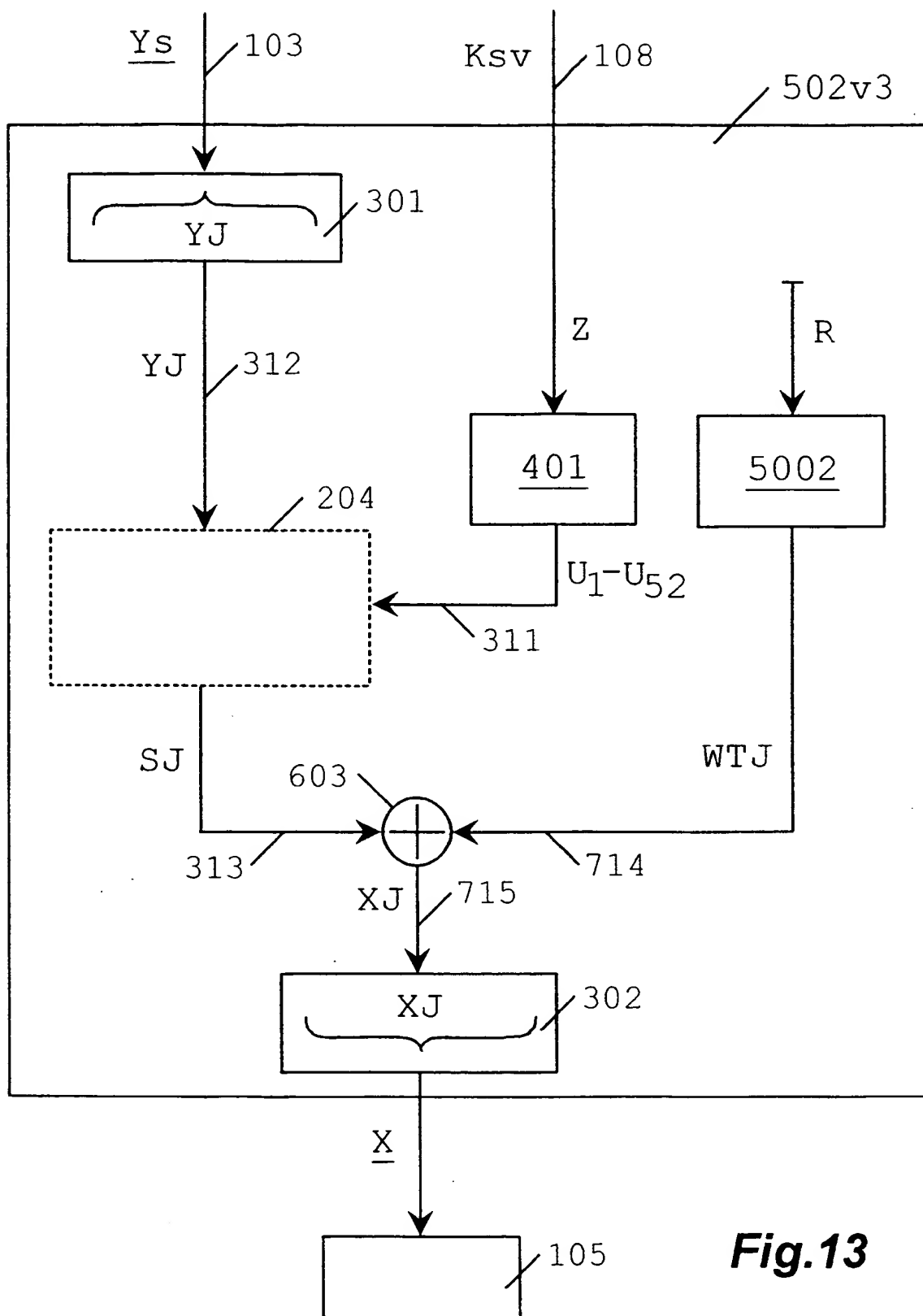
10/12

**Fig.11**

11/12

**Fig.12**

12/12

**Fig.13**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/ ES 99/ 00115A. CLASSIFICATION OF SUBJECT MATTER ⁶:

IPC6 H04L9/20 H04L9/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6 H04L, G09C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CIBEPAT, WPI, EPODOC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9633564 A1 (SECURE COMPUTING CORPORATION) 24 October 1996 (24.10.96), See the whole document	1-4, 23-26
A	EP 877509 A2 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 11 November 1998 (11.11.98), See the whole document	1-4, 23-26
A	US 5479513 A (PROTOPODESCU ET AL.) 26 December 1995 (26.12.95), See the whole document	1-4, 23-26
A	EP 635956 A2 (CANON KABUSHIKI KAISHA) 25 January 1995 (25.01.95), See the whole document	1-4, 23-26
A	EP 4467239 A2 (HUGHES AIRCRAFT COMPANY) 22 January 1992 (22.01.92), See the whole document	1-4, 23-26
A	US 3798360 A (FEISTEL) 19 March 1974 (19.03.74), See the whole document	1-4, 23-26



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
26 August 1999 (26.08.99)Date of mailing of the international search report
15 September 1999 (15.09.99)Name and mailing address of the ISA/
S.P.T.O

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/ ES 99/ 00115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9633564 A1	24.10.1996	JP 10508450T T US 5796836 A EP 0821853 A1 AU 5542896 A	18.08.1998 18.08.1998 04.02.1998 07.11.1996
EP 877509 A2	11.11.1998	JP 10327141 A GB 2325123 A	08.12.1998 11.11.1998
US 54795133 A	26.12.1995	NONE	
EP 635956 A2	25.01.1995	AU 693444 B US 5600720 A CA 2128115 A AU 6754594 A JP 7038558 A JP 7036672 A	02.07.1998 04.02.1997 21.01.1995 02.02.1995 07.02.1995 07.02.1995
EP 467239 A2	22.01.1991	US 5048086 A DE 69118977T T DE 69118977D D JP 4250490 A	10.09.1991 19.09.1996 30.05.1996 07.09.1992
US 3798360 A	19.03.1974	IT 956497 B JP 54025785B B GB1351572 A FR2143971 AB DE2231835 ABC	10.10.1973 30.08.1979 01.05.1974 09.02.1973 11.01.1973

INFORME DE BÚSQUEDA INTERNACIONAL

Solicitud internacional nº
PCT/ES 99/00115

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

CIP⁶ H04L9/20, H04L9/28

De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y la CIP.

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima consultada (sistema de clasificación, seguido de los símbolos de clasificación)

CIP⁶ H04L, G09C

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

CIBEPAT, WPI, EPODOC, PAJ

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría*	Documentos citados, con indicación, si procede, de las partes relevantes	Relevante para las reivindicaciones nº
A	WO 9633564 A1 (SECURE COMPUTING CORPORATION) 24.10.1996, todo el documento.	1-4, 23-26
A	EP 877509 A2 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 11.11.1998, todo el documento.	1-4, 23-26
A	US 5479513 A (PROTOPODESCU ET AL.) 26.12.1995, todo el documento.	1-4, 23-26
A	EP 635956 A2 (CANON KABUSHIKI KAISHA) 25.01.1995, todo el documento.	1-4, 23-26
A	EP 4467239 A2 (HUGHES AIRCRAFT COMPANY) 22.01.1992, todo el documento.	1-4, 23-26
A	US 3798360 A (FEISTEL) 19.03.1974, todo el documento.	1-4, 23-26

☐ En la continuación del recuadro C se relacionan otros documentos ☐ Los documentos de familia de patentes se indican en el anexo

* Categorías especiales de documentos citados:

- *A* documento que define el estado general de la técnica no considerado como particularmente relevante.
- *E* solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.
- *L* documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada).
- *O* documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio.
- *P* documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.

T documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención.

X documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.

Y documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

& documento que forma parte de la misma familia de patentes.

Fecha en que se ha concluido efectivamente la búsqueda internacional. 26.08.1999

Fecha de expedición del informe de búsqueda internacional

15 SEP 1999

(15.09.99)

Nombre y dirección postal de la Administración encargada de la búsqueda internacional O.E.P.M.

C/Panamá 1, 28071 Madrid, España.
nº de fax +34 91 3495304

Funcionario autorizado

BOTELLA MALDONADO, JAIME
nº de teléfono + 34 91 349 5393

INFORME DE BÚSQUEDA INTERNACIONAL

Información relativa a miembros de familias de patentes

Solicitud internacional n°

PCT/ES 99/00115

Documento de patente citado en el informe de búsqueda	Fecha de Publicación	Miembro(s) de la Familia de patentes	Fecha de Publicación
WO 9633564 A1	24.10.1996	JP 10508450T T US 5796836 A EP 0821853 A1 AU 5542896 A	18.08.1998 18.08.1998 04.02.1998 07.11.1996
EP 877509 A2	11.11.1998	JP 10327141 A GB 2325123 A	08.12.1998 11.11.1998
US 54795133 A	26.12.1995	NINGUNO	
EP 635956 A2	25.01.1995	AU 693444 B US 5600720 A CA 2128115 A AU 6754594 A JP 7038558 A JP 7036672 A	02.07.1998 04.02.1997 21.01.1995 02.02.1995 07.02.1995 07.02.1995
EP 467239 A2	22.01.1991	US 5048086 A DE 69118977T T DE 69118977D D JP 4250490 A	10.09.1991 19.09.1996 30.05.1996 07.09.1992
US 3798360 A	19.03.1974	IT 956497 B JP 54025785B B GB1351572 A FR2143971 AB DE2231835 ABC	10.10.1973 30.08.1979 01.05.1974 09.02.1973 11.01.1973